

**NETWORK INTERCONNECTING DEVICE****Publication number:** WO9713345**Publication date:** 1997-04-10**Inventor:** SATOH HIROSHI (JP); OGAWA TETSUO (JP)**Applicant:** KAWASAKI STEEL CO (JP); SATOH HIROSHI (JP);  
OGAWA TETSUO (JP)**Classification:****- international:** *H04L12/46; H04L12/56; H04L12/46; H04L12/56; (IPC1-7): H04L12/46***- European:** H04L12/46B; H04L12/56; H04L12/56C3**Application number:** WO1996JP02873 19961003**Priority number(s):** JP19950257334 19951004; JP19950353590 19951229**Also published as:**

US6065064 (A1)

**Cited documents:**

JP3289839



JP5219060



JP63039231



JP5022295

**Report a data error here****Abstract of WO9713345**

A network interconnecting device has two stages, a mask processing section (10) and a transmission control information generating section (30). The mask processing section (10) generates an address mask for extracting various kinds of address components from the destination address (IP) contained in a received message in accordance with the address (IP). Therefore, the extraction of various kinds of address components such as the network address and sub-network address is simplified.

---

Data supplied from the **esp@cenet** database - Worldwide



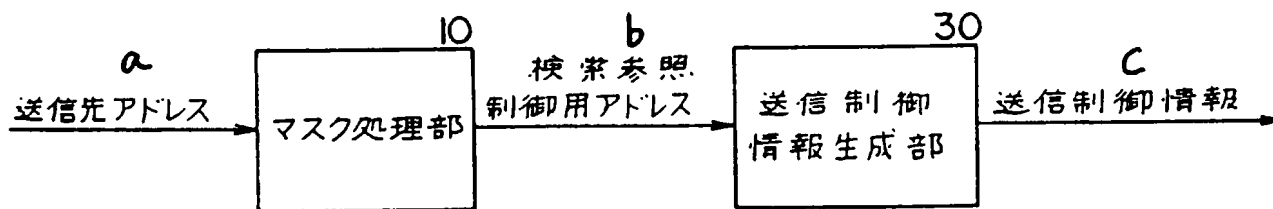
PCT

特許協力条約に基づいて公開された国際出願

<p>(51) 国際特許分類6 H04L 12/46</p>	<p>A1</p>	<p>(11) 国際公開番号 WO97/13345</p> <p>(43) 国際公開日 1997年4月10日(10.04.97)</p>
<p>(21) 国際出願番号 PCT/JP96/02873</p> <p>(22) 国際出願日 1996年10月3日(03.10.96)</p> <p>(30) 優先権データ 特願平7/257334 1995年10月4日(04.10.95) JP 特願平7/353590 1995年12月29日(29.12.95) JP</p> <p>(71) 出願人 (米国を除くすべての指定国について) 川崎製鉄株式会社(KAWASAKI STEEL CORPORATION)[JP/JP] 〒651 兵庫県神戸市中央区北本町通一丁目1番28号 Hyogo, (JP)</p> <p>(72) 発明者：および</p> <p>(75) 発明者／出願人 (米国についてのみ) 佐藤 宏(SATOH, Hiroshi)[JP/JP] 小川哲男(OGAWA, Tetsuo)[JP/JP] 〒100 東京都千代田区内幸町二丁目2番3号 川崎製鉄株式会社 東京本社内 Tokyo, (JP)</p> <p>(74) 代理人 弁理士 高矢 論, 外(TAKAYA, Satoshi et al.) 〒151 東京都渋谷区代々木二丁目10番4号 新宿辻ビル Tokyo, (JP)</p>		<p>(81) 指定国 JP, US.</p> <p>添付公開書類 国際調査報告書</p>

(54)Title: NETWORK INTERCONNECTING DEVICE

(54)発明の名称 ネットワーク間接続装置



a ... destination address

b ... retrieval-reference controlling address

c ... transmission control information

10 ... mask processing section

30 ... transmission control information generating section

(57) Abstract

A network interconnecting device has two stages, a mask processing section (10) and a transmission control information generating section (30). The mask processing section (10) generates an address mask for extracting various kinds of address components from the destination address (IP) contained in a received message in accordance with the address (IP). Therefore, the extraction of various kinds of address components such as the network address and sub-network address is simplified.

## (57) 要約

ネットワーク間接続装置を、マスク処理部(10)と送信制御情報生成部(30)との2段構成とする。マスク処理部(10)では、受信したメッセージ中の送信先アドレス(IP)から各種アドレス成分を抽出するためのアドレスマスクを、該送信先アドレス(IP)に従って生成する。これにより、受信したメッセージの送信先アドレス(IP)から、ネットワークアドレスやサブネットワークアドレス等の各種アドレス成分を抽出する処理の簡便化を図る。

## 情報としての用途のみ

PCTに基づいて公開される国際出願をパンフレット第一頁にPCT加盟国を同定するために使用されるコード

AL	アルバニア	EE	エストニア	LR	リベリア	RU	ロシア連邦
AM	アルメニア	ES	スペイン	LS	レソト	SD	スーダン
AT	オーストリア	FI	フィンランド	LT	リトアニア	SE	スウェーデン
AU	オーストラリア	FR	フランス	LU	ルクセンブルグ	SG	シンガポール
AZ	アゼルバイジャン	GA	ガボン	LV	ラトヴィア	SI	スロベニア
BB	バルバドス	GB	イギリス	MC	モナコ	SK	スロバキア共和国
BE	ベルギー	GE	グルジア	MD	モルドバ	SN	セネガル
BG	ブルガリア	GH	ガーナ	MG	マダガスカル	SZ	スワジランド
BJ	ベナン	GN	ギニア	MK	マケドニア	TD	チュニジア
BR	ブラジル	GR	ギリシャ	VI	ベトナム	TG	トーゴ
BY	ベラルーシ	HU	ハンガリー	ML	マリ	TJ	タジキスタン
CA	カナダ	IE	アイアランド	MN	モンゴル	TM	トルクメニスタン
CF	中央アフリカ共和国	IT	イタリア	MR	モーリタニア	TR	トルコ
CG	コンゴ	JP	日本	MW	マラウイ	TT	トリニダード・トバゴ
CH	スイス	KE	ケニア	MX	メキシコ	UG	ウガンダ
CI	コート・ジボアール	KG	キルギスタン	NE	ニジェール	US	米国
CM	カメルーン	KP	朝鮮民主主義人民共和国	NL	オランダ	UZ	ウズベキスタン共和国
CN	中国	KR	韓国	NO	ノルウェー	VN	ベトナム
CZ	チェコ共和国	KZ	カザフスタン	NZ	ニュージーランド	YU	ユーゴスラビア
DE	ドイツ	LI	リヒテンシュタイン	PL	ポーランド		
DK	デンマーク	LK	スリランカ	PT	ポルトガル		
				RO	ルーマニア		

## 明細書

### ネットワーク間接続装置

#### 技術分野

本発明は、物理層から上位へ各階層がそれぞれ定義された、複数のプロトコル階層に従ったプロトコルのメッセージをそれぞれ伝送する、複数のネットワーク間に配置され、特定のプロトコル階層でこれらネットワーク間を接続する機能を有し、異なるネットワークにある送信元から送信先へ、送信先アドレスのデータを含むメッセージを送信するために用いられるネットワーク間接続装置に係る。特に、受信したメッセージ（受信フレーム）の送信先アドレスからネットワークアドレスやサブネットワークアドレスを抽出するなどの、従来複雑で処理時間を要していた処理を中心として、ループ処理を低減したり、又、比較的簡単な処理に置き換えたりすることで、ネットワーク間接続装置における送信経路決定処理などの諸処理を能率よく行えるようにし、これによって、処理速度の向上や、利用するハードウェアの簡略化でコスト削減を図ると共に、装置全体のハードウェア化も可能とすることができるネットワーク間接続装置に関する。

#### 背景技術

電話型公衆通信回線等の電話網や特定通信回線等、音声による相互通信を目的として構築された電話網は、データ通信に利用しようとする伝送品質や伝送速度の面で制約がある。このため、データトラフィック特性等、データ通信特有の特性に、より適合したデジタルデータ公衆網の構築が、日本を含め世界各国で進められている。このデジタルデータ公衆網は、デジタル信号用の伝送路及び交換機を用いたものであり、日本では、回線交換網やパケット交換網によるサービスが提供されている。又、国際接続についても、CCITT (international telegraph and telephone consultative committee) によって国際標準化が進められ、現在、回線交換方式、パケット交換方式、デジタル専用線等、新データ網関係の勧告（Xシリーズ勧告）としてほぼ整備されている。

一方、データベースなどの情報（データ）や周辺機器の共有等を目的として、近年、LAN（Local Area Network）と称するネットワークが広く用いられるようになってきている。このLANは、限定された所定の構内、例えばオフィスや工場や研究所、大学等の限定された範囲内で、分散設置されたコンピュータや通信端末機器等のデジタル機器を接続するものであり、ある種の交換機能を有している。このようなLANにおいても、IEEE（Institute of Electrical Electronic s Engineers）802委員会や、ISO（International Standardization Organization；国際標準化機構）等において、プロトコル等の標準化が行われている。

デジタルデータ公衆網で適用されているOSI（Open Systems Interconnection）参照モデルや、IEEEで標準化された前述のようなLANのプロトコルは、物理層から上位へ各階層がそれぞれ定義される、複数のプロトコル階層によって定義されている。又、WAN（Wide Area Network）や他のLAN等で広く用いられるプロトコルについても、通常複数のプロトコル階層に従って定義されている。このように、大抵のネットワークのプロトコルは、複数のプロトコル階層に従って定義されている。

又、LANやWANあるいはデジタルデータ公衆網等、複数のネットワーク間を接続することが従来から行われている。例えば、伝送するメッセージのプロトコルを定義する複数のプロトコル階層のうち、少なくとも幾つかの階層が相互に異なるネットワーク間でも、従来からネットワーク間接続が行われている。

ここで、OSI第2層のMAC（Media Access Control）層が同一の2つのネットワークを第2層で接続するネットワーク間接続装置は、ブリッジ等と呼ばれている。OSI第1層～第7層が異なる複数のネットワークを接続するネットワーク間接続装置は、ゲートウェイ等と呼ばれている。又、本願の後述する実施形態として言及されているような、OSI第1層～第3層が異なる複数のネットワークを第3層で接続するネットワーク間接続装置は、ルータ等と呼ばれている。

なお、本願発明が対象とするネットワーク間接続装置は、後述する実施形態のルータに限定されるものではなく、例えば前述のブリッジやゲートウェイにも適用することができる。又、本発明が適用されたネットワーク間接続装置が接続す

るネットワークについても、前述した特定のLANに限定されるものではなく、種々のLANやWAN、デジタルデータ公衆網であってもよい。

ここで、従来から用いられている、LAN間を接続するネットワーク間接続装置、特にIP (Internet Protocol) ルータについて、本願発明に係る部分をより詳細に説明する。

IPルータは、受信フレームに含まれるIPヘッダ中の送信先IPアドレスに基づいて、この受信フレームの送信経路を決定する処理 (IPルーティング処理と称する) を行う。このようなIPルーティング処理は、送信先IPアドレスの各種アドレス成分、特に、ネットワークアドレスを抽出しながら実行される。

なお、一般的なネットワーク間接続装置においても、受信したメッセージ中の送信先アドレスから各種アドレス成分を抽出し、該各種アドレス成分に従った制御を行いながら、当該ネットワーク間接続装置に接続される送信先側の該当するネットワークへ、受信したメッセージを転送する一連の処理 (ルーティング処理と称する) が行われている。

前記送信先IPアドレスは、32ビット構成とされ、図1に示されるように、クラスビット、ネットワークアドレスビット、及び、ホストアドレスビットの合計3つのフィールドから構成されている。又、各フィールドは、この順に、32ビットのIPアドレスのMSB (Most Significant Bit) 側からLSB (Least Significant Bit) 側へ構成されている。図1に示されるように、クラスビットで示されるA～Cのアドレスクラスに応じて、該クラスビットのフィールドのビット数を含め、ネットワークアドレスビットのフィールドのビット数、及び、ホストアドレスビットのフィールドのビット数が決定される。

図1に示されるように、まず、32ビットのIPアドレスのMSBが“0”である場合、クラスビットで“A”のアドレスクラス (クラスAと称する) が示される。この場合、ネットワークアドレスビットのフィールドは7ビット、ホストアドレスビットのフィールドは24ビットとなる。又、IPアドレスのMSBから2つのビットが“10”の場合、クラスビットで“B”のアドレスクラス (クラスBと称する) が示される。この場合、ネットワークアドレスビットのフィールドは14ビット、ホストアドレスビットのフィールドは16ビットとなる。又、

I PアドレスのMSBから3つのビットが“110”の場合、クラスビットで“C”のアドレスクラス（クラスCと称する）が示される。この場合、ネットワークアドレスビットのフィールドは21ビット、ホストアドレスビットのフィールドは8ビットとなる。

前記ネットワークアドレスは、インターネット上の各ネットワークのアドレスを示す。該ネットワークアドレスは、前記クラスビットとネットワークアドレスビットで表わされる。ホストアドレスは、前記ネットワークアドレスで示されるネットワーク内において、個々のホストのアドレスを示す。このホストアドレスは、前記ホストアドレスビットで表わされる。

前記I Pルータは、複数のネットワーク間に配置され、各ネットワークから受け取る受信フレーム中に含まれるI Pヘッダ中の送信先I Pアドレスを検査する。該I Pルータは、送信先I Pアドレスの特にネットワークアドレスを調べ、該ネットワークアドレスが、そのI Pルータのポート（自ポート）に接続されているネットワークであるならば、そのI PアドレスのホストアドレスからMACアドレスを引き出し、該当するホストに対してフレームを送信する。一方、I Pアドレス中のネットワークアドレスが、自ポートに接続されるネットワーク以外のアドレスを示している場合には、その受信フレームを他ポートへ中継する。

32ビットのI Pアドレスからネットワークアドレスを抽出する際に、I Pルータは、受信フレームのI Pアドレスマスクの処理を行う。このマスク処理は、I Pアドレスと所定のアドレスマスクの対応するビット同士の論理積を演算することによって行われる。ここで、アドレスマスクは、I Pアドレスと同じ32ビットのデータである。特にネットワークアドレスを抽出するためのアドレスマスクでは、I Pアドレスのクラスビットとネットワークアドレスビットのフィールドと同じビット位置の各ビットが“1”であり、その他、I Pアドレス中のホストアドレスビットフィールドと同じビット位置の各ビットは“0”となる。

前記アドレスマスクは、I Pアドレス等の送信先アドレスとの論理積で、ネットワークアドレス等の各種アドレス成分を抽出するよう用いられる。このため、アドレスマスクのビットが“1”であれば、その桁で特定のアドレス成分のビットの抽出を行うが、このように抽出対象とすることを、以降、「マスクする」と

表現する。一方、“0”であれば、このような特定のアドレス成分の抽出を行わないが、このように非対象とすることを以降、「マスクしない（無視）」と表現する。

IPアドレスが、このようにクラスA～クラスCの3種類のみであれば、ネットワークアドレスビットのフィールドの種類も3種類のみであり、従って、ネットワークアドレスビットを抽出するために用いるアドレスマスクも3種類備えておけばよい。実際にネットワークアドレスを抽出する際には、IPアドレスのMSBから1つ～3つのビットによって、アドレスクラスがクラスA～クラスCのいずれであるか判定し、これに応じて3種類のアドレスマスクを選択し、選択したアドレスマスクを用いてネットワークアドレスビットを抽出すればよく、比較的簡単に自動的に行うことができる。

しかしながら、近年では、IPアドレスが枯渇するとともに、32ビットで表わされるアドレスをより有効に利用することが要求されている。このため、ホストアドレスビットの最初の数ビットを、ネットワークアドレスビットに準ずるものとして、1つのネットワークを複数に分割したサブネットワークのアドレス指定に用いるマルチプロトコル処理が行われるようになってきている。

前記IPルータが、このようなマルチプロトコルのサブネットワーク間に設置された場合、アドレスマスクを用いた前記ネットワークアドレスを抽出する処理に類似した、サブネットワークアドレスを抽出する処理を行い、受信フレームから抽出したサブネットワークアドレスに従って正しく中継する必要がある。又、このようにサブネットワークアドレスを抽出するためには、専用のアドレスマスクを備える必要がある。

従って、近年のIPルータは、接続されるネットワークのネットワークアドレスやサブネットワークアドレスに対応するため、IPアドレスのみならず、これに対するアドレスマスクと対でテーブルを有している。このようなテーブルを用いて、受信フレームのIPアドレス中のネットワークアドレスやサブネットワークアドレスを抽出している。このようにテーブルを用いる方法は、論理的には簡潔であり理解しやすいが、実際の処理に当たっては、次に示すような複雑な問題を内包している。



即ち、サブネットワークアドレスのフィールドがIPアドレスに無い場合、表1を用いて前述したように、受信フレームに含まれるIPアドレスのMSBから1つ～3つのビットからアドレスクラスを判定し、ネットワークアドレスを抽出するためのアドレスマスクを一義的に求めることができる。しかしながら、サブネットワークアドレスのフィールドがIPアドレスに存在する場合、サブネットワークアドレスやネットワークアドレスを抽出するためのアドレスマスクを一義的に求めることができない。このため、IPルータにおいては、一般に以下の処理のどちらかを実行する必要がある。

A1. IPルータ内のテーブル中のネットワークアドレス（テーブル内のIPアドレスをアドレスマスクにてマスク処理したもの）と、受信フレーム中のIPアドレスとを比較し、テーブル内の全エントリ中で、最も多くのビットがIPアドレスと一致したものを選択し、そのエントリのネットワークアドレスを送信先として使用する処理。

A2. 受信フレーム中のIPアドレスに対するアドレスマスクが全ビット“1”としてマスク処理を行い、テーブル中のネットワークアドレスと比較する。一致するものが無い場合は、アドレスマスクのLSBを“0”として、再び、テーブル中のネットワークアドレスと比較する。このとき、更に一致するものが無かった場合には、アドレスマスクのLSB側から次のビットも“0”として、再びテーブル中のネットワークアドレスと比較する。このように、一致するものが見出されるまで、アドレスマスクのビットを、LSB側から1ビットずつ逐次“0”としながら、このようなテーブル中のネットワークアドレスとの比較を行う処理。

上記のA1やA2の処理のように、従来は、サブネットワークアドレスのフィールドがIPアドレスに存在するマルチプロトコルの場合、ネットワークアドレスを抽出する処理が非常に複雑になってしまい、処理時間も大きくなってしまいうという問題があった。又、このような処理は、一般にソフトウェアでしか実行することができず、ハードウェア化することが極めて困難であるという問題があった。更に、ネットワークアドレスの抽出後も、32ビットでそのまま検索できるテーブルを備えることは、テーブルのデータ数が大きくなる等不経済である。従って、専用の論理回路を外部に設け、ハッシュ関数を用いてツリー状にデータを

検索するハッシュ等の措置が必要となり、ソフトウェアの負担を大きくしてしまう。

このため、処理時間を短縮するべく高性能なCPU（Central Processing Unit）を使用するのが一般的である。しかしながら、高性能なCPUを用いたとしても処理時間の短縮には限界があり、このようなネットワークアドレスの抽出の処理や、該抽出の後になされるテーブル検索の処理は、IPルータにおける中継処理のボトルネックとなっていた。

又、処理を簡略化するべく、連想メモリ（Contents Addressable Memory ; CAM）の利用を考えても、マスクのビット長が変わるため、対応するビット長毎にCAMが必要となり、メリットが生かせなかった。

#### 発明の開示

本発明は、前記従来の問題点を解決するべくなされたもので、受信したメッセージ（受信フレーム）の送信先アドレスからネットワークアドレスやサブネットワークアドレスを抽出するなどの、従来複雑で処理時間を要していた処理を中心として、ループ処理を低減したり、又、比較的簡単な処理に置き換えたりすることで、ネットワーク間接続装置における送信経路決定処理などの諸処理をマルチプロトコルに対応して能率よく行えるようにし、これによって、処理速度の向上や、利用するハードウェアの簡略化によるコスト削減を図ることを課題とする。

本発明は、物理層から上位へ各階層がそれぞれ定義された、複数のプロトコル階層に従ったプロトコルのメッセージをそれぞれ伝送する、複数のネットワーク間に配置され、特定のプロトコル階層でこれらネットワーク間を接続する機能を有し、異なるネットワークにある送信元から送信先へ、送信先アドレスのデータを含むメッセージを送信するために用いられるネットワーク間接続装置において、当該ネットワーク間接続装置が受信したメッセージ中の前記送信先アドレスから各種アドレス成分を抽出するためのアドレスマスクを、該送信先アドレスに従って生成すると共に、生成した該アドレスマスクで前記送信先アドレスを処理した検索参照制御用アドレスを出力するマスク処理部と、該検索参照制御用アドレスに基づき、当該ネットワーク間接続装置での送信先側のネットワークへのメッセ

ージ送信の際に用いる送信制御情報を生成する送信制御情報生成部とを備え、該送信制御情報に従って、当該ネットワーク間接続装置に接続される送信先側の該当するネットワークへ、受信したメッセージを転送するようにして、前記課題を解決したものである。

又、前記マスク処理部を、参照用エントリアドレスと、該参照用エントリアドレスの個々のビットが前記各種アドレス成分の抽出に関与するか否かを示す参照用エントリマスクとの対を、アドレスエントリデータとして複数記憶するアドレスマスクテーブルと、対応する前記アドレスエントリデータについて、その参照用エントリマスクでマスクをかけながら、その参照用エントリアドレスと前記送信先アドレスとのアドレス一致を判定する、前記アドレスエントリデータと同数だけ設けられるエントリデータ比較器と、これらエントリデータ比較器のうち、アドレス一致と判定したそれぞれのエントリデータ比較器に対応するアドレスエントリデータの参照用エントリマスクを合成しながら、実際に用いる前記アドレスマスクを生成するアドレスマスク生成部と、該アドレスマスクで前記送信先アドレスを処理して前記検索参照制御用アドレスを生成し、出力するマスキング回路とで構成することにより、ループ処理を排し、高速なハードウェアでの実現を可能としたものである。なお、ループ処理の一部を残すこともできる。

更に、前記アドレスマスク生成部が、前記エントリデータ比較器のうち、アドレス一致と判定したそれぞれのエントリデータ比較器に対応するアドレスエントリデータの参照用エントリマスクの中で、前記各種アドレス成分の抽出に関与することが指定されたビットの数が最も多い参照用エントリマスクを選択し、これを前記アドレスマスクとして出力するようにしたものである。

又、前記参照用エントリマスクが、マスク長を示すデータによって、前記各種アドレス成分の抽出に関与する前記参照用エントリアドレスの個々のビットを示すようにして、前記アドレスマスクテーブルに複数あるアドレスエントリデータの特に前記参照用エントリマスクのビット長を短縮することで、前記アドレスマスクテーブルの小型化を可能としたものである。

更に、前記アドレスエントリデータが全ビット有効フラグを有すると共に、前記エントリデータ比較器が、前記アドレス一致の判定の際に、当該エントリデー

タ比較器に対応する前記アドレスエントリデータの前記全ビット有効フラグが有効を示している場合、前記アドレスマスク生成部が用いる参照用エントリマスクの全ビットを強制的に有効にセットする機能を実現する全マスクビット強制セット回路を有するようにして、当該ネットワーク間接続装置に直接接続されているコンピュータホストと、当該ネットワーク間接続装置に他のネットワーク間接続装置を介して接続されているコンピュータホストの両方に対してデータフレームを中継する場合に必要となる、送信先アドレスのマスク処理の多様性についても対応可能としたものである。

又、前記送信制御情報生成部が、前記送信制御情報を記憶する連想メモリを備え、前記検索参照制御用アドレスを該連想メモリの検索データとし、該連想メモリのデータ一致のアドレス出力を用いて前記送信制御情報を生成するようにして、前記送信制御情報生成部の動作を能率良く行えるようにし、その動作速度の向上などを図ったものである。

又、前記送信制御情報生成部が、前記送信制御情報を記憶する連想メモリを備え、前記検索参照制御用アドレスを該連想メモリの検索データとし、該連想メモリのデータ一致が検出されたアドレスにより指し示されるデータの内、検索に使用されなかった部分のデータを用いて前記送信制御情報を生成するようにして、前記送信制御情報生成部の動作を能率良く行えるようにし、その動作速度の向上等を図ったものである。

又、前記アドレスエントリデータと同数だけ設けられる複数のエントリデータ比較器の全てにおいてアドレス一致が検出されなかった場合に、前記送信先アドレスのビット列の判定により該送信先アドレスのアドレスクラスを認識し、該アドレスクラスに基づいて、前述の各種アドレス成分の抽出に関与するか否かをビット毎に指定するビット列を生成し、該ビット列を前記アドレスマスクとして使用するようにして、前記アドレスエントリデータのデータ数を削減することを可能とし、又、より広範囲のネットワークへの対応を容易にしたものである。

本発明は、又、前記のようなネットワーク間接続装置において、当該ネットワーク間接続装置が受信したメッセージ中の前記送信先アドレスから各種アドレス成分を抽出するための、異なる複数のアドレスマスクを、マスクする桁数が多い

ものから少ないものへ順に記憶するマスクレジスタ群と、該マスクレジスタ群に記憶される複数のアドレスマスクを、マスクする桁数が多いものから少ないものへ順に選択するために用いるカウンタと、前記各種アドレス成分にて示される送信経路のそれぞれのアドレスを検索データとして記憶し、前記カウンタで選択されたアドレスマスクを用いながら、前記送信先アドレスに一致する前記アドレスを検索し、一致するものが存在する場合にはヒット信号を出力すると共に、一致した検索データが記憶される連想メモリアドレスをヒットアドレス信号として出力する連想メモリと、前記カウンタの初期化の制御を行うと共に、該カウンタで順次カウントすることで、マスクする桁数が多いものから少ないものへ順にアドレスマスクを選択しながら前記ヒット信号が出力されるまでなされる、前記連想メモリを用いた検索の制御を行う検索シーケンサとを備え、前記ヒットアドレス信号に基づいて識別される、当該ネットワーク間接続装置に接続される送信先側の該当するネットワークへ、受信したメッセージを転送するようにして、前記課題を解決するとともに、ハードウェアでの実現を可能としたものである。

又、前記アドレスマスク群、前記カウンタ、及び前記連想メモリを複数組備え、複数の前記アドレスマスク群それぞれに、順に輪番に、異なる複数の前記アドレスマスクを、マスクする桁数が多いものから少ないものへ、一つずつ順にふり分けて記憶し、複数の前記連想メモリに、相互に同一の前記検索データを記憶するようにして、検査処理の並列実行により、処理速度の向上を可能としたものである。

以下、本発明の作用について、図を用いて簡単に説明する。

まず、前提として、本発明のネットワーク間接続装置は、物理層から上位へ各階層がそれぞれ定義された、複数のプロトコル階層に従ったプロトコルのメッセージ、例えば受信フレームをそれぞれ伝送する、複数のネットワーク間に配置されている。又、本発明のネットワーク間接続装置は、特定のプロトコル階層でこれらネットワーク間を接続する機能を有し、異なるネットワークにある送信元から送信先へ、送信先アドレスのデータを含むメッセージを送信するために用いられる。

又、本発明のネットワーク間接続装置の一例は、基本的に、図2に示されるよ

うに、マスク処理部10と、送信制御情報生成部30とを備えている。

まず、マスク処理部10は、当該ネットワーク間接続装置が受信したメッセージ中の前記送信先アドレスから各種アドレス成分を抽出するためのアドレスマスクを、該送信先アドレスに従って生成するとともに、生成した該アドレスマスクで前記送信先アドレスを処理した、検索参照制御用アドレスを出力する。この検索参照制御用アドレスは、従来技術で前述した、受信フレームの送信先IPアドレスから抽出されるネットワークアドレスやサブネットワークアドレスに相当する。又、本発明のこのマスク処理部10の特徴は、前記送信先アドレスから各種アドレス成分を抽出するためのアドレスマスクを、該送信先アドレスに従って生成している点にある。即ち、従来技術として前述したIPルータの如く、単にクラスビットに従ってアドレスマスクを生成するのではなく、より積極的に、前記送信先アドレスに従ってアドレスマスクを生成している。

次に、前記送信制御情報生成部30は、前記マスク処理部10で出力される前記検索参照制御用アドレスに基づき、当該ネットワーク間接続装置での送信先のネットワークへのメッセージ送信の際に用いる、送信制御情報を生成する。

例えば、前述したマスク処理部10が出力する前記検索参照制御用アドレスが、従来技術で前述したようなネットワークアドレスやサブネットワークアドレスである場合、該送信制御情報生成部が出力する送信制御情報は、当該ネットワーク間接続装置において受信したメッセージを転送送信するためのネットワークが接続されているポートの番号や、MACアドレスであってもよい。あるいは、例えば、前述のマスク処理部10が生成する前記検索参照制御用アドレスが、従来技術として言及したネットワークアドレスやサブネットワークアドレスを生成する前処理に用いる予備的な信号である場合、該送信制御情報生成部30が出力する前記送信制御情報を、ネットワークアドレスやサブネットワークアドレスとしてもよい。

このように、本発明においては、受信したメッセージ（例えば受信フレーム）中の送信先アドレスから、従来技術で言及したようなネットワークアドレスやサブネットワークアドレスを抽出したり、更には送信するメッセージ（フレーム）を送り出すネットワークのポート番号やMACアドレスを生成する処理に際し、

前述のようなマスク処理部１０と送信制御情報生成部３０との独特な２段階構成を取ることによって、能率の良い処理を行うことができる。又、特にマスク処理部１０についても、送信先アドレスから各種アドレス成分を抽出するためのアドレスマスクを送信先アドレスに従って生成するという、独特の処理を行っているため、アドレスマスクを生成するという従来困難であった処理を改善することができる。

なお、本発明はこれに限定されるものではないが、前述の送信制御情報生成部３０において、連想メモリを用いるようにしてもよい。本発明は、前述のように特にマスク処理部１０と送信制御情報生成部３０との２段階構成となっているため、このような連想メモリも容易に用いることができる。又、このように連想メモリを用いた場合、送信制御情報生成部３０において、例えば、受信したメッセージの送信先アドレスから前記マスク処理部１０で抽出された各種アドレス成分を中心として、入力する信号に従って、ネットワークアドレスやサブネットワークアドレス、その他、関係するネットワークのポート番号やＭＡＣアドレス等の生成をより能率良く行うことができ、処理速度の向上や、利用するハードウェアの簡略化によるコスト削減等を図ることができる。

又、本発明のネットワーク間接続装置の他の例は、基本的に、図３に示される如く、マスクレジスタ群１２２と、カウンタ１２４と、ＣＡＭ１１６と、検索シーケンサ１１２とを備えている。

まず、マスクレジスタ群１２２は、当該ネットワーク間接続装置が受信したメッセージ中の送信先ＩＰアドレスＩＰから、各種アドレス成分を抽出するための異なる複数のアドレスマスクを、マスクする桁数が多いものから少ないものへ順に記憶する。即ち、該マスクレジスタ群１２２は、マスクする桁数が多く、従ってマスクされない桁数が少ないものから、マスクする桁数が少なく、従ってマスクされない桁数が多いものへ、順に、異なる複数のアドレスマスクを記憶している。

前記カウンタ１２４は、前記マスクレジスタ群１２２に記憶される複数のアドレスマスクを、マスクする桁数が多いものから少ないものへ順に選択するために用いられる。該カウンタ１２４は、検索初期化信号ＩＮＴでカウント値が初期化

されると、マスクする桁数が最も多く、従ってマスクされない桁数が最も少ないアドレスマスクを指し示す選択信号SEを出力する。又、該カウンタ124は、検索開始信号STが入力される毎に、そのカウント値を“1”だけ変更し、インクリメント（“1”だけ値を増加）あるいはデクリメント（“1”だけ値を減少）する。これによって、該カウンタ124は、検索開始信号STが入力される毎に、マスクする桁数が多いものから少ないものへ順に選択するための選択信号SEを出力する。

前記CAM116は、各種アドレス成分で示される送信経路のそれぞれのアドレスを検索データとして記憶する。この送信経路のアドレスとは、当該ネットワーク間接続装置の送信先側にあるネットワークや別のネットワーク間接続装置等を示すアドレスであり、例えば前述した、受信フレームの送信先IPアドレスから抽出されるネットワークアドレスやサブネットワークアドレスに相当する。該CAM116は、前述のカウンタ124が出力する選択信号SEによって選択された、マスクレジスタ群122から出力される選択マスク信号SM（アドレスマスク）を用いながら、送信先IPアドレスIPに一致する、当該CAM116に記憶される前述のようなアドレスを検索する。このような検索に際し、一致するものが存在する場合には、該CAM116は、該一致有りを示すヒット信号HTを少なくとも検索シーケンサ112へ出力するとともに、一致した検索データが記憶される連想メモリアドレスをヒットアドレス信号HAとして出力する。この検索データは、前述のような送信経路の該当するものを示すアドレスである。

前記検索シーケンサ112は、外部から送信先IPアドレスIPが入力されると、まず検索初期化信号INTを出力することでカウンタ124の初期化の制御を行う。この後、該検索シーケンサ112は、CAM116からヒット信号HTが入力されるまで、逐次、検索開始信号STをカウンタ124へ出力する。本発明のネットワーク間接続装置では、このように検索開始信号STを逐次カウンタ124へ入力し、該カウンタ124で順次カウント（カウントアップ又はカウントダウン）することで、マスクする桁数が多いものから少ないものへ順に、マスクレジスタ群122に記憶されるアドレスマスクを選択して得られる選択マスク信号SMを得ると共に、該選択マスク信号SMを用いながら、CAM116にお



ける検索を、ヒット信号HTが出力されるまで行う。

以上説明したような図3に示される構成、即ちマスキレジスタ群122、カウンタ124、CAM116及び検索シーケンサ112によれば、入力される送信先IPアドレスIPに応じたヒットアドレス信号HAを得ることができる。又、該ヒットアドレス信号HAに基づいて識別される、当該ネットワーク間接統装置に接続される送信先側の該当するネットワーク等を認識することができる。従って、該ネットワーク間接統装置では、このようにして得られるヒット信号HTを用いながら、該ネットワーク間接統装置に接続される送信先側の該当するネットワークへ、受信したメッセージを転送することができる。

従って、本発明によれば、受信したメッセージ（受信フレーム）の送信先アドレスからネットワークアドレスやサブネットワークアドレスを抽出するなどの、従来複雑で処理時間を要していた処理を中心として、ループ処理を低減したり、又、比較的簡単な処理に置き換えたりすることで、ネットワーク間接統装置における送信経路決定処理などの諸処理を能率よく行えるようにし、これによって、処理速度の向上や、利用するハードウェアの簡略化でコスト削減を図ると共に、装置全体のハードウェア化も可能とすることができる。

#### 図面の簡単な説明

図1は、32ビット構成の送信先IPアドレスを示す図表である。

図2は、本発明の基本的な構成の一例を示すブロック図である。

図3は、本発明の基本的な構成の他の例を示すブロック図である。

図4は、本発明が適用されたネットワーク間接統装置の第1実施形態の構成を示すブロック図である。

図5は、第1実施形態に用いられるマスク処理部の構成を示すブロック図である。

図6は、第1実施形態に用いられるアドレスマスクテーブルを構成するアドレスエントリデータの構造を示す線図である。

図7は、第1実施形態のマスク処理部に用いられるエントリデータ比較器の構成を示すブロック図である。

図8は、第1実施形態の処理手順を示す流れ図である。

図9は、本発明が適用されたネットワーク間接統装置が運用されるネットワーク環境を示したブロック図である。

図10は、前記ネットワーク間接統装置のアドレスマスクテーブルの設定例を示す図表である。

図11は、前記ネットワーク間接統装置の送信制御情報生成部に備えられた連想メモリ上に設定される送信制御情報の例を示す図表である。

図12は、本発明が適用されたネットワーク間接統装置の第2実施形態の構成を示すブロック図である。

図13は、第2実施形態に用いるCAMシーケンサの内部構成を示すブロック図である。

図14は、前記CAMシーケンサのマスクレジスタ群に記憶されたアドレスマスクの一部を示す図表である。

図15は、本発明が適用されたネットワーク間接統装置の第3実施形態の構成を示すブロック図である。

図16は、第3実施形態に用いる一方のCAMシーケンサのマスクレジスタ群に記憶されたマスクデータの例を示す線図である。

図17は、他方のCAMシーケンサのマスクレジスタ群に記憶されたマスクデータの例を示す図表である。

図18は、上記2つのマスクレジスタ群の対応関係を示す図表である。

#### 発明を実施するための最良の形態

以下、図を用いて本発明の実施の形態を詳細に説明する。

図4は、本発明が適用されたネットワーク間接統装置の第1実施形態の構成を示すブロック図である。

図4に示されるように、本第1実施形態は、マスク処理部10Aと、送信制御情報を記憶する連想メモリ（CAM）30Bを供えた送信制御情報生成部30Aとによって構成されている。

前記マスク処理部10Aは、本実施形態のネットワーク間接統装置が受信した

受信フレーム（メッセージ）中の送信アドレスとして、送信先IPアドレスIPAを入力し、該送信先IPアドレスIPAから各種アドレス成分を抽出するためのアドレスマスクを生成するとともに、生成したアドレスマスクで送信先IPアドレスIPAを処理したマスク済IPアドレスIPM（検索参照制御用アドレス）を出力する。

前記CAM30Aは、前記マスク処理部10Aから入力されたマスク済IPアドレスIPMに基づき、連想メモリ30Bを利用して、当該ネットワーク間接続装置での送信先側のネットワークへのフレーム送信（メッセージ送信）の際に用いるMACアドレス／ポート番号PD（送信制御情報）を生成する。本実施形態のネットワーク間接続装置では、このように生成されたMACアドレス／ポート番号PDに従って、当該ネットワーク間接続装置に接続される、送信先側の該当するネットワークへ、受信したフレームを転送する。

図5は、本第1実施形態に用いられる前述のマスク処理部の構成を示すブロック図である。

この図5に示されるマスク処理部10Aは、連想メモリ30Bに格納された、合計 $(m+1)$ 個のアドレスエントリデータ $T_0 \sim T_m$ を有するアドレスマスクテーブルTBと、合計 $(m+1)$ 個のエントリデータ比較器 $CP_0 \sim CP_m$ と、OR回路14及び16と、アドレスクラスマスク生成回路18と、セクタ20と、マスキング回路22とにより構成されている。

前記連想メモリ30Bに格納されたアドレスマスクテーブルTBが備える合計 $(m+1)$ 個のアドレスエントリデータ $T_0 \sim T_m$ のそれぞれは、図6に示されるように、1ビットのデータ有効フラグEFと、同じく1ビットの全ビット有効フラグAFと、32ビットの参照用エントリマスクRMと、同じく32ビットの参照用エントリアドレスRAとにより構成されている。

前記データ有効フラグEFは、そのアドレスエントリデータ $T_0 \sim T_m$ が有効か否かを示す。このデータ有効フラグEFは、有効であれば“1”となり、無効であれば“0”となる。

前記全ビット有効フラグAFは、主として前述のエントリデータ比較器の後述するセクタ44で用いられるものであり、参照用エントリマスクRMの内容に

かかわらず、アドレスマスクのすべてのビットを“1”に強制的に設定する、全ビット有効であるか否かを示す。この全ビット有効フラグAFは、このような全ビット有効の場合、“1”となり、有効ではない場合“0”となる。

前記参照用エントリアドレスRAは、アドレスマスクを決定する際に、後述のエントリデータ比較器CPO～CPmにより、送信先IPアドレスIPAと比較される。参照用エントリマスクRMは、前述の送信先IPアドレスIPAとの比較の際に、該参照用エントリマスクに対応するエントリデータ比較器CPO～CPmにより使用される。即ち、該参照用エントリマスクに対応する参照用エントリアドレスRAと送信先IPアドレスIPAは、該参照用エントリマスクに“1”が設定されているビットに対応するビット位置については一致比較の対象となり、該一致比較の結果が、該参照用エントリアドレスRAと送信先IPアドレスIPA全体の比較結果に反映されるが、該参照用エントリマスクに“0”が設定されているビットに対応するビット位置については一致比較の対象とならず、該一致比較の結果は、該参照用エントリアドレスRAと送信先IPアドレスIPA全体の比較結果に反映されない。

前記エントリデータ比較器CPO～CPm（以降、エントリデータ比較器CPと総称する）は、図7を用いて後述するような内部構成となっている。又、これらエントリデータ比較器CPは、それぞれ該当するアドレスエントリデータTO～Tmから、参照用エントリマスクRM及び参照用エントリアドレスRAを入力する（合計64ビット）。又、これらエントリデータ比較器CPは、いずれも、送信先IPアドレスIPAを入力する。このエントリデータ比較器CPは、入力される参照用エントリマスクRMでマスクをかけながら、入力される参照用エントリアドレスRAと送信先IPアドレスIPAとのアドレス一致を判定する。

一致し、かつ、該当するアドレスエントリデータのデータ有効フラグEFが“1”と判定された場合（アドレス一致）、エントリヒット信号EH（EH0～EHm）として、“1”を出力する。又、このようにアドレス一致と判定された場合には、これらエントリデータ比較器CPそれぞれは、参照用エントリマスクRM及び全ビット有効フラグAFに従ってエントリマスクデータ信号EMを出力する。即ち、一致が検出され且つデータ有効フラグEFが“1”であるエントリの

エントリデータ比較器は、当該アドレスエントリデータの全ビット有効フラグAFが“0”の場合には、当該アドレスエントリデータのエントリマスクRMをエントリマスクデータ信号EMとして出力する。一方、当該アドレスエントリデータの全ビット有効フラグAFが“1”の場合には、全ビットに“1”が設定されたビット列をエントリマスクデータ信号EMとして出力する。

なお、アドレス一致でないと判定された場合、エントリマスクデータ信号EMの値は“0”（すべてのビットが“0”）となる。

前記OR回路14は、合計 $(m+1)$ 個の入力を有する多入力OR回路である。このOR回路14は、エントリデータ比較器CPそれぞれが出力するエントリヒット信号EH（EH0～EHm）をそれぞれ入力し、これらの論理和を演算し、この結果をテーブルヒット信号THとして、セクタ20の選択信号Sに出力する。

前記OR回路16は、 $(m+1)$ の入力を有する多入力OR回路を合計32個用いて構成されている。これらの多入力OR回路は、エントリデータ比較器CPそれぞれが出力するエントリマスクデータ信号EMの32ビットそれぞれに対応して配置されている。又、これら多入力OR回路は、合計 $(m+1)$ 個の入力それぞれへ、合計 $(m+1)$ 個のエントリデータ比較器CPそれぞれの出力するエントリマスクデータ信号EM（EM0～EMm）の同一の該当ビットを入力し、論理和演算を行う。このような合計 $(m+1)$ 個の多入力OR回路によって、OR回路16は、32ビットのマスクデータ信号EAを出力する。このマスクデータ信号EAの32ビットの各ビットは、32個の多入力OR回路それぞれに対応している。

前記アドレスクラスマスク生成回路18は、送信先IPアドレスIPAのMSBからの1つ～3つのビットに従って、前述の表1に示されたA～Cのアドレスクラスを判定するとともに、該判定に従って、ネットワークアドレスを抽出するためのアドレスマスクとして、マスクデータ信号EBを出力する。このマスクデータ信号EBは32ビットである。

前記セクタ20は、OR回路14が出力するテーブルヒット信号THに従って、OR16が出力するマスクデータ信号EA又はアドレスクラスマスク生成回

路18が出力するマスクデータ信号EBのいずれか一方を選択する。即ち、このセクタ20は、テーブルヒット信号THが“1”であればマスクデータ信号EAを選択し、テーブルヒット信号THが“0”であればマスクデータ信号EBを選択する。選択されたものは、32ビットのマスクデータ信号ECとして出力される。

前記マスキング回路22は、セクタ20が出力するマスクデータ信号ECに従って、送信先IPアドレスIPAに対してマスキング処理を行う。即ち、このマスキング回路22は、32ビットのマスクデータ信号ECと、同じく32ビットの送信先IPアドレスIPAとについて、同一ビット同士で論理積の演算を行い、同一ビット位置のマスク済IPアドレスIPMのビットの値を決定し、このようにしながら32ビットのマスク済IPアドレスIPMを生成し、出力する。より具体的には、このマスキング回路22は、マスクデータ信号EC及び送信先IPアドレスIPAの同一ビットどうしについて、マスクデータ信号EC側のビットが“0”であれば、マスク済IPアドレスIPMの同一ビット位置のビットを“0”とする。又、このマスキング回路22は、マスクデータ信号EC及び送信先IPアドレスIPAについて、マスクデータ信号EC側のビットが“1”であれば、同一ビット位置のマスク済IPアドレスIPMのビットへと送信先IPアドレスIPAの同一ビット位置のビットの値を出力する。

図7は、本実施形態に用いられるエントリデータ比較器の内部構成を示すブロック図である。

この図7に示される如く、本実施形態で前述のように合計(m+1)個用いられるエントリデータ比較器CPは、いずれも、合計32個のエクスクルーシブNOR回路E0～E31と、合計32個のインバータI0～I31と、合計32個のOR回路R0～R31と、多入力AND回路42と、セクタ44と、合計32個のAND回路A0～A31とにより構成されている。

前記エクスクルーシブNOR回路E0～E31（以降、エクスクルーシブNOR回路Eと総称する）は、いずれも、2入力であり、これら2つの入力へ入力される論理値が一致する場合“1”を出力する。従って、これらエクスクルーシブNOR回路Eは、一方の入力が“1”で、かつ、他方の入力が“0”の場合には、

“0”を出力する。

前記インバータI0～I31は、いずれも一般的なインバータであり、入力した論理値を反転させて出力する。前記OR回路R0～R31は、論理和の演算を行う、一般的な2入力のものである。前記多入力AND回路42は、32本の入力を有し、これらの入力の論理積を演算し、この演算結果をエントリヒット信号EHとして出力する。

従って、エクスクルーシブNOR回路E0～E31と、インバータI0～I31と、OR回路R0～R31と、多入力AND回路42とによって、次のような演算がなされる。

まず、エクスクルーシブNOR回路E0～E31それぞれによって、参照用エントリアドレスRAと送信先IPアドレスIPAとの同一ビット位置同士の論理値の比較がなされ、一致する場合“1”が出力され、不一致の場合“0”が出力される。又、OR回路R0～R31は、これらエクスクルーシブNOR回路E0～E31の出力と、インバータI0～I31を経て入力される参照用エントリマスクRMとの同一ビット位置同士の論理和の演算を行う。

従って、これらOR回路R0～R31のそれぞれは、該当する参照用エントリマスクRMのビットが“1”の場合には、該当するエクスクルーシブNOR回路E0～E31で反転された一致／不一致の判定結果を出力する。一方、OR回路R0～R31のそれぞれは、該当する参照用エントリマスクRMのビットが“0”の場合には、エクスクルーシブNOR回路E0～E31の一致／不一致の判定結果にかかわらず、常に“1”を出力する。

又、このようにして出力されるOR回路R0～R31のすべての出力に対して、又、データ有効フラグEFに対して、多入力AND回路42によって論理積の演算がなされ、この結果がエントリヒット信号EHとして出力される。

従って、これらエクスクルーシブNOR回路E0～E31、インバータI0～I31、OR回路R0～R31及び多入力AND回路42によって、参照用エントリマスクRMでマスクをかけながら、参照用エントリアドレスRAと送信先IPアドレスIPAとのアドレス一致の判定がなされ、一致と判定された場合エントリヒット信号EHが“1”となり、不一致と判定された場合にはエントリヒッ

ト信号EHは“0”となる。

次に、セクタ44は、入力Sに“0”が入力されていると、32個の入力を有する入力PAを選択する。一方、該セクタ44は、入力に“1”が入力されていると、32個の入力を有する入力PBを選択する。従って、該セクタ44は、全ビット有効フラグAFが“0”であれば参照用エントリマスクRMを選択し、全ビット有効フラグAFが“1”であれば、32ビットのすべての出力から“1”を出力する。

次に、AND回路A0～A31は、いずれも一方の入力に、多入力AND42が出力するエントリヒット信号EHが入力されている。又、これらAND回路A0～A31は、セクタ44が他方の入力へ出力する32ビットの信号のうちから、該当する1ビットが入力されている。これらAND回路A0～A31からは、エントリマスクデータ信号EMが出力される。

従って、エントリヒット信号EHが“1”の場合、エントリマスクデータ信号EMの値は、セクタ44が選択した値となり、即ち、参照用エントリマスクRMの値、あるいは32ビットのすべてのビットが“1”となる値となる。一方、エントリヒット信号EHが“0”の場合、エントリマスクデータ信号EMの値は“0”（全てのビットが“0”）となる。

本実施形態における基本的な処理手順をまとめて図8に示す。

本実施形態は、以上説明した如く、ハードウェアによって構成することができ、又、ソフトウェアによっても構成することができる。本実施形態をハードウェアで構成した場合、各部の動作を並行あるいはほぼ並行に動作させ、処理速度の向上等を図ることも可能である。例えば、ハードウェアで構成する際、前述の合計 $(m+1)$ 個のエントリデータ比較器CP0～CPmを相互に独立動作可能に構成すれば、これらでなされる処理を互いに並行して実行することができる。このため、アドレスマスクテーブルTBが有する多数 $((m+1)$ 個)のアドレスエントリデータと、送信先IPアドレスIPAとの比較を並行して行うことができ、処理速度の向上を図ることが可能である。

本実施形態で図6を用いて前述した参照用エントリマスクRMや参照用エントリアドレスRAは、32ビットのビット長のデータとして記憶されている。しか



し、これら参照用エントリマスクRM及び参照用エントリアドレスRAは、このような32ビットのビットパターンを、32ビットのビット長で記憶するものに限定されるものではない。例えば、32ビットのビットパターンで、“1”や“0”が多数連続することが考えられる場合、ランレングスのようなもので記憶してもよい。特に、参照用エントリマスクRMについては、“1”又は“0”が連続するビットパターンとなることが多いため、ランレングスを用いたデータによって記憶すれば、該参照用エントリマスクRMに要するビット数を削減でき、結果として、アドレスエントリデータのデータ（ビット数）を削減し、アドレスマスクテーブルTBのデータ（ビット数）も削減することができる。

又、本実施形態では、セクタ20が参照用エントリマスクを選択するようにされていたが、マスク済みIPアドレスを直接選択するようにしても良い。次に、本発明の実際のネットワークにおける動作について、図面を参照して説明する。図9は、本発明が適用されたネットワーク間接続装置が運用されるネットワーク環境を示したブロック図である。

本発明が適用されたネットワーク間接続装置は、図9中ではネットワーク間接続装置1として示されている。該ネットワーク間接続装置1は、PID=1からPID=3の3つのポートを有しており、PID=1のポートには“133. 190. 52. xx”のIPアドレスを持つサブネットワーク1が、PID=2のポートには“133. 190. 51. xx”のIPアドレスを持つサブネットワーク2が、PID=3のポートには、もう1台のネットワーク間接続装置であるネットワーク間接続装置2が、それぞれ接続されている。同様に、ネットワーク間接続装置2は、PID=1からPID=3の3つのポートを有しており、PID=1のポートには前記ネットワーク間接続装置1が、PID=2のポートには“133. 190. 53. xx”のIPアドレスを持つサブネットワーク3が、PID=3のポートには“133. 191. xx. xx.”のIPアドレスを持つネットワークが、それぞれ接続されている。ここで、IPアドレスの上位桁“133. 190.”等がネットワークアドレスを示し、下位桁“52. xx”等がホストアドレスを示す。

“133. 190. 52. xx”のIPアドレスを持つサブネットワーク1に

は、コンピュータ1からコンピュータ3の3台のコンピュータが接続されている。同様に、“133. 190. 51. xx”のIPアドレスを持つサブネットワーク2には、コンピュータ4からコンピュータ6の3台のコンピュータが、“133. 190. 53. xx”のIPアドレスをもつサブネットワーク3には、コンピュータ7からコンピュータ9の3台のコンピュータが、“133. 191. x x. x x”のIPアドレスを持つネットワークには、コンピュータ10からコンピュータ12の3台のコンピュータが、それぞれ接続されている。

ここで注目したいのは、“133. 190. x x. x x”はクラスBのIPアドレスであり、本来であれば“255. 255. 0. 0”のマスクが適用されるべきものであるが、サブネットワークアドレスとして8ビット拡張し、“255. 255. 255. 0”のマスクが適用されており、更にそのサブネットワーク境界にネットワーク間接続装置が設けられている点である。今日のネットワーク構築に際して、このようなマルチプロトコルの手法は極めて一般的であり、これがネットワーク間接続装置における処理を複雑なものにしている。

図10は、図9におけるネットワーク間接続装置1のアドレスマスクテーブルTBの設定例を示す。但し、当該表にある“NO.”の項は、説明を容易とするために敢えて設けたものであり、実際の例においては必要のないものである。

図11は、図9におけるネットワーク間接続装置1の前記送信制御情報生成部の連想メモリ上に設定される送信制御情報の例を示す。但し、当該表にある“NO.”の項は、説明を容易とするために敢えて設けたものであり、実際の例においては必要のないものである。

次に実際の動作例を説明する。

まず、コンピュータ7がコンピュータ1にデータを送信する際に、当該データをネットワーク間接続装置1がPID=3のポートから受信した後の動作について説明する。

ネットワーク間接続装置1は、受信したデータの送信先IPアドレスが“133. 190. 52. 201”であることを知り、これを当該装置内のマスク処理部10Aに入力する。

マスク処理部10Aは、図10に示すアドレスマスクテーブルTBを用いて、

この送信先IPアドレスに対するマスク処理を行う。この例においては、図10のNO. 2のアドレスエントリデータにおいて一致が検出され、該アドレスエントリデータの全ビット有効フラグAFが“1”にセットされていることから、該送信先IPアドレスの全ビットがそのままマスク済みIPアドレスIPMとして、前記連想メモリ30Aに出力される。即ち、前記連想メモリ30Aに出力されるマスク済みIPアドレスIPMは、“133. 190. 52. 201”である。

前記連想メモリ30Aは、当該マスク済みIPアドレスIPMを検索のキーデータとして、図11に示す送信制御情報のIPアドレスのフィールドを検索する。その結果として、NO. 4のエントリで一致が検出され、当該エントリのMACアドレスのフィールドを読み出すことにより、当該データの最終受信先であるコンピュータ1のMACアドレス“02698C 0AC49D”を得ると共に、PIDのフィールドを読み出すことにより、ネットワーク間接続装置1が当該データを出力するポートPID=1を得ることができる。

次に、コンピュータ1がコンピュータ7にデータを送信する際に、当該データをネットワーク間接続装置1がPID=1のポートから受信した後の動作について説明する。

ネットワーク間接続装置1は、受信したデータの送信先IPアドレスが“133. 190. 53. 201”であることを知り、これを当該装置内のマスク処理部10Aに入力する。

マスク処理部10Aは、図10に示すアドレスマスクテーブルTBを用いて、この送信先IPアドレスに対するマスク処理を行う。この例においては、図10のNO. 3のアドレスエントリデータにおいて一致が検出され、該アドレスエントリデータの全ビット有効フラグAFが“0”にセットされていること、及び、該アドレスエントリデータの参照用エントリマスクRMが“255. 255. 255. 0”に設定されていることにより、送信先IPアドレスの上位24ビットはそのまま、下位8ビットが“0”に設定されたビット列が、マスク済みIPアドレスIPMとして、前記連想メモリ30Aに出力される。即ち、前記連想メモリ30Aに出力されるマスク済みIPアドレスIPMは、“133. 190. 53. 0”である。

前記連想メモリ30Aは、当該マスク済みIPアドレスIPMを検索のキーデータとして、図11に示す送信制御情報のIPアドレスのフィールドを検索する。その結果として、NO. 7のエントリで一致が検出され、当該エントリのMACアドレスのフィールドを読み出すことにより、当該データの次の送信先であるネットワーク間接統装置2のMACアドレス“02698C 0AC502”を得ると共に、PIDのフィールドを読み出すことにより、ネットワーク間接統装置1が当該データを出力するポートPID=3を得ることができる。

次に、コンピュータ1がコンピュータ12にデータを送信する際に、当該データをネットワーク間接統装置1がPID=1のポートから受信した後の動作について説明する。

ネットワーク間接統装置1は、受信したデータの送信先IPアドレスが“133. 191. 53. 203”であることを知り、これを当該装置内のマスク処理部10Aに入力する。

マスク処理部10Aは、図10に示すアドレスマスクテーブルTBを用いて、この送信先IPアドレスに対するマスク処理を行う。この例においては、どのアドレスエントリデータにおいても一致が検出されないため、アドレスクラス認識に基づいてマスク処理が行われる。“133. 191. 53. 203”のIPアドレスはクラスBであるため、送信先IPアドレスの上位16ビットはそのまま、下位16ビットが“0”に設定されたビット列が、マスク済みIPアドレスIPMとして、前記連想メモリ30Aに出力される。即ち、前記連想メモリ30Aに出力されるマスク済みIPアドレスIPMは、“133. 191. 0. 0”である。

前記連想メモリ30Aは、当該マスク済みIPアドレスIPMを検索のキーデータとして、図11に示す送信制御情報のIPアドレスのフィールドを検索する。その結果として、NO. 10のエントリで一致が検出され、当該エントリのMACアドレスのフィールドを読み出すことにより、当該データの次の送信先であるネットワーク間接統装置2のMACアドレス“02698C 0AC502”を得ると共に、PIDのフィールドを読み出すことにより、ネットワーク間接統装置1が当該データを出力するポートPID=3を得ることができる。

図12は、本発明が適用されたネットワーク間接続装置の第2実施形態の構成を示すブロック図である。

本実施形態のネットワーク間接続装置は、前記第1実施形態と同様に、TCP/IPに代表されるネットワークプロトコルを処理する中継機能を有するネットワーク機器であり、IPアドレスを用いて、受信フレームのIPルーティング処理を行うIPルータである。

本実施形態における、IPルーティング処理を行い、受信フレームに含まれる送信先IPアドレスから送信先のポート番号、及びMACアドレスを決定するルーティング機能部は、図12に示される如く、検索シーケンサ112Lと、CAM116Lと、CAMシーケンサ114Lとにより構成されている。

前記検索シーケンサ112Lは、送信先IPアドレスIPAを入力し、当該送信先IPアドレスIPAを送信先IPアドレスIPBとしてCAM116Lに送出する機能を有する。又、該検索シーケンサ112Lは、CAM116L及びCAMシーケンサ114Lに対して、送信先IPアドレスIPAに基づいた連想記憶のテーブル検索を指示する検索開始信号STを送出する。該検索シーケンサ112Lは、CAMシーケンサ114Lに対して、検索の初期化を指示する検索初期化信号INTを送出する。該検索シーケンサ112Lにおいては、CAM116Lが出力するヒット信号HTを入力し、該ヒット信号HTに基づき、次のテーブル検索を指示するか否かを判断する。このように、検索シーケンサ112Lにおいては、送信先IPアドレスIPAを入力し、又ヒット信号HTを入力しながら、送信先IPアドレスIPB、検索開始信号ST及び検索初期化信号INTを出力することで、本実施形態における一連のテーブル検索の制御を行う。

該検索シーケンサ112Lは、基本的には図3を用いて前述した検索シーケンサ112と同等である。即ち、該検索シーケンサ112Lにおいても、CAMシーケンサ114Lが内蔵するカウンタ124Lの初期化の制御を行う。又、該検索シーケンサ112Lは、カウンタ124Lで順次カウントすることで、マスクする桁数が多いものから少ないものへ順にアドレスマスク（選択マスクとなるもの）を選択しながらヒット信号HTが出力されるまでなされる、CAM116Lを用いた連想メモリの検索の制御を行う。

前記CAM116Lは、基本的なCAMの構成のデータテーブルを有する。このデータテーブルは、各種アドレス成分にして示される送信経路のそれぞれのアドレスを、検索データとして記憶したものである。該CAM116Lは、当該データテーブル内の各エントリに格納されているデータと、送信先IPアドレスIPBとの一致比較を、CAMシーケンサ114Lから入力される選択マスク信号SMで伝達される選択マスク（アドレスマスク）に従って、全てのエントリに対して同時に実行する。ここで、前記選択マスクは、一致比較を行うべきビット位置を指定するものであり、図14、図16、図17を用いて後述するような形態である。このような一致比較に際し、データテーブル内に送信先IPアドレスIPBに一致するエントリが存在する場合にはヒット信号HTが“1”となり、一致が検出されたエントリの当該CAM116Lのアドレスを示すヒットアドレス信号HAが出力される。一方、このような一致比較に際して送信先IPアドレスIPBと一致するエントリが存在しない場合には、ヒット信号HTは“0”となる。該CAM116Lは、基本的には、図3を用いて前述したCAM116に相当する。

次にCAMシーケンサ114Lは、図13に示されるような構成となっており、カウンタ124Lと、セクタ126と、マスクレジスタ群122Lとを備えている。該CAMシーケンサ114Lは、前述した図3のカウンタ124とマスクレジスタ群122とを含む機能を有している。

図13において、マスクレジスタ群122Lには、受信したメッセージ中の送信先IPアドレスIPAから各種アドレス成分を抽出するための、合計m個の異なるアドレスマスクが記憶されている。該マスクレジスタ群122Lのこのような合計m個のアドレスマスクは、図14に示される如く、マスクビットが“1”となっているマスクする桁数が多いものから少ないものへ、従ってマスクビットが“0”となっているマスクされない桁数が少ないものから多いものへ順に記憶されている。

図13において、カウンタ124Lは、検索初期化信号INTにより初期化され、検索開始信号STによりインクリメントされるアップカウンタである。該カウンタ124Lは、マスクレジスタ群122Lに記憶される合計m個のアドレス

マスクを、セクタ126を用いて、マスクする桁数が多いものから少ないものへ順に選択するために用いられる選択信号SEを出力する。該選択信号SEに基づいてセクタ26が選択したアドレスマスクは、該選択マスク信号SMとして出力される。

以下、第2実施形態の作用について説明する。

前記検索シーケンサ112Lは、送信先IPアドレスIPAが入力されると、該送信先IPアドレスIPAと同一の送信先IPアドレスIPBをCAM116Lへ送信する。該送信と同時に、検索シーケンサ112Lは、CAMシーケンサ114Lに対して“1”の検索初期化信号INTを送出する。該CAMシーケンサ114L内のカウンタ124Lは、検索初期化信号INTが入力されると初期化され、該カウンタ124Lのカウント値は“0”となる。又、このような初期化により、該カウンタ124Lから出力される選択信号SEは“0”となる。すると、選択信号SEの値の番号のマスクデータを選択するセクタ126は、マスクレジスタ群122Lから出力される合計m個のマスクデータ、即ちマスクデータ0～マスクデータ(m-1)の中からマスクデータ0を選択し、これを選択マスク信号SMとして出力する。

次に、検索シーケンサ112Lは、“1”の検索開始信号STをCAM116Lへ出力する。これにより、該CAM116Lは、送信先IPアドレスIPBを検索キーデータとし、当該CAM116L内のデータテーブルの全エントリ内のデータを検索対象とし、セクタ126から出力される選択マスク信号SMをマスクデータとして用いるマスク処理を行いながら、1回目の連想記憶の検索動作を起動する。

CAM116Lは、検索開始信号STの立上がりエッジにより、送信先IPアドレスIPBと選択マスク信号SMとをラッチし、ラッチした選択マスク信号SMの“1”となっているマスクビットのビット位置に対して、ラッチしたIPBアドレスと、データテーブル内の全てのエントリに格納されているデータとの一致比較を行う。一致するエントリがある場合には、ヒット信号HTが“1”となり、一致したエントリのCAM116Lにおけるアドレスであるヒットアドレス信号HAを出力する。一方、一致するエントリが無い場合には、ヒット信号HT

は“0”となる。

検索シーケンサ112Lは、CAM116Lからのヒット信号HTが“1”であれば、再び検索動作の起動を行うことはない。一方、ヒット信号HTが“0”の場合には、検索シーケンサ112Lは再度検索開始信号STを送出し、2回目の検索動作を起動する。

ここで、検索開始信号STは、上述のようにCAM116Lへ送出されているだけでなく、CAMシーケンサ114Lに対しても送出されている。該CAMシーケンサ114Lにおいては、1回目の検索動作を起動した検索開始信号STの立ち下がりエッジにより、該CAMシーケンサ114Lが内蔵するカウンタ124Lのカウントアップ（インクリメント）が行われる。これにより、セクタ126は、第2回目の検索動作に備えてマスクデータ1を選択し、これを選択マスク信号SMとして出力する。この選択マスク信号SMは、2回目の検索動作を起動する検索開始信号STの立ち上がりエッジで、CAM116Lにラッチされる。又、このように選択マスク信号SMがラッチされると、CAM116Lは、マスクデータ1を用いた2回目の検索動作を実行する。

2回目の検索動作の後、CAM116Lが“0”のヒット信号HTを出力すれば、検索シーケンサ112Lは、再び検索開始信号STを送出し、これにより3回目の検索動作が起動される。3回目の検索動作が起動されると、CAM116Lは、マスクレジスタ群122Lのマスクデータ2が選択して得られた選択マスク信号SMを用いて、再び検索動作を行う。このようにして、CAM116Lが出力するヒット信号HTが“1”となるまで、マスクレジスタ群122Lに記憶されるm個のマスクデータを選択しながら検索実行がなされる。

なお、このように順次選択されるマスクレジスタ群122Lのマスクデータは、図14に示した如く、マスクする桁数が多いものから少ないものへと順に選択される。

1回目の検索に用いられるマスクデータ0には、マスクビットの32ビット全てが“1”であるマスクデータが設定されている。従って、1回目の検索動作においては、32ビット長の送信先IPアドレスIPB（送信先IPアドレスIPA）の全ビットを検索対象とする検索動作がCAM116Lで実行される。



2回目の検索動作に用いられるマスクデータ1には、図14のマスクデータ1に示される如く、LSBのマスクビットが“0”で、それ以外のマスクビットが“1”であるマスクデータが設定されている。従って、2回目の検索動作においては、LSBを除くその他のビットを検索対象とする、送信先IPアドレスIPB（送信先IPアドレスIPA）の検索動作が実行される。

検索動作がこのように繰り返されるにつれて、選択マスク信号SMに選択されるマスクデータが1ビットずつ変化し、検索対象となるビットと、検索対象にされないビットとの境界が1ビットずつMSB側へと移行する。これによって、IPアドレス内のネットワークアドレスビットとホストアドレスビットとの境界をLSB側から1ビットずつずらして検索を行うことに対応し、境界をLSB側から開始することにより、IPルーチング処理において最も適切なネットワークアドレスビットを抽出することが可能となる。

本第2実施形態のルーチング機能部でも、第1実施形態と同様に、本発明が適用されたIPルーチング処理を行うことができる。

図15は、本発明が適用されたネットワーク間接続装置の第3実施形態の構成を示すブロック図である。

本実施形態のネットワーク間接続装置は、前記第1、第2実施形態と同様に、TCP/IPに代表されるネットワークプロトコルを処理する中継機能を有するネットワーク機器であり、IPアドレスを用いて受信フレームのIPルーチング処理を行うIPルータである。

本実施形態における、受信フレームに含まれる送信先IPアドレスIPAから送信先のポート番号及びMACアドレスを決定するIPルーチング処理を行うルーチング機能部は、検索シーケンサ112Aと、CAM116A及び116Bと、CAMシーケンサ114A及び114Bとを備えている。

本実施形態の検索シーケンサ112Aは、第2実施形態の検索シーケンサ112Lに相当する。又、第2実施形態のCAMシーケンサ114L及びCAM116Lでなされる機能が、本実施形態では、CAMシーケンサ114A及びCAM116Aで構成される部分と、CAMシーケンサ114B及びCAM116Bで構成される部分とを用い、これら2つの部分それぞれでの処理を並行実行しなが

らなされるようになっている。本実施形態では、このようにCAMシーケンサ114A及び114Bと、CAM116A及び116Bとの組み合わせが2対ある構成となっている。

前記検索シーケンサ112Aは、送信先IPアドレスIPAが入力されると、第1実施形態の検索シーケンサ112Lと同様に、検索初期化信号INT及び送信先IPアドレスIPBを出力する。本実施形態の検索シーケンサ112Aでは、CAM116Aが出力するヒット信号HTAが“0”であり、且つ、CAM116Bが出力するヒット信号HTBが“0”である間、1回目、第2回目等と、逐次“1”の検索開始信号STを出力し、順次検索動作を続行する。

前記CAM116A及び116Bは、いずれも、第2実施形態のCAM116Lと同一のものとなっている。CAM116Lのヒット信号HT及びヒットアドレス信号HAが、CAM116Aのヒット信号HTA及びヒットアドレス信号HAAとなり、CAM116Bのヒット信号HTB及びヒットアドレス信号HABとなっている。

前記CAMシーケンサ114A及び114Bは、基本的には、第2実施形態の図13に示される構成のCAMシーケンサ114Lと同一のものとなっている。CAMシーケンサ114A及び114Bのカウンタ124L及びセクタ126は、CAMシーケンサ114Lのカウンタ124L及びセクタ126と同一である。しかしながら、本実施形態のCAMシーケンサ114Aのマスキレジスタ群122Lは、図16のように合計m個のマスキデータを記憶しており、CAMシーケンサ114Bのマスキレジスタ群122Lは、図17のように合計n個のマスキデータを記憶している。ここで、 $(n \times 2)$ はmと等しく、CAM116AとCAM116Bに記憶される全マスキデータの個数 $(n \times 2)$ は、CAMシーケンサ114Lに記憶されるマスキデータの個数mと等しい。

ここで、図16と図17のマスキデータは、図18に示す如く、マスキデータ番号が同一のものどうしが組とされ、同一のタイミングでなされるCAM116Aあるいは116Bにおける検索動作に用いられる。

本実施形態においては、検索シーケンサ112Aが出力する1つの検索開始信号STによる1回の検索動作により、CAMシーケンサ114A及びCAM11

6Aを用いた検索動作と、CAMシーケンサ114B及びCAM116Bを用いた検索動作とが並行実行され、異なる2種類のマスクデータによる異なる選択マスク信号SMA及びSMBを用いた、同一の送信先IPアドレスIPB（送信先IPアドレスIPA）に対する検索動作が実行される。CAM116Aと116Bのデータテーブル上のデータは同一のものであっても、使用されるアドレスマスクに対応して異なったものであってもよい。

図16及び図17の例では、1回目の検索動作において、CAMシーケンサ114Aは、マスクビット32ビットの全てが“1”であるマスクデータを選択マスク信号SMAとして出力する。一方、CAMシーケンサ114Bは、マスクビットLSBが“0”でそれ以外のマスクビットが全て“1”であるマスクデータを選択マスク信号SMBとして出力する。

又、2回目の検索動作においては、CAMシーケンサ114Aは、LSB側から2つのマスクビットが“0”で、これ以外のマスクビットが“1”であるマスクデータを選択マスク信号SMAとして出力する。一方、CAMシーケンサ114Bは、LSB側から3つのマスクビットが“0”で、これ以外のマスクビットが全て“1”であるマスクデータを、選択マスク信号SMBとして出力する。

検索シーケンサ112Aは、CAM116Aが出力するヒット信号HTA、及びCAM116Bが出力するヒット信号HTBの少なくともいずれか一方が“1”になるまで、逐次検索開始信号STを出力し、検索動作を繰り返し起動する。

ここで、CAM116Aのヒット信号HTAと、CAM116Bのヒット信号HTBとが同時に“1”となることも考えられる。このような場合で、特に、CAMシーケンサ114Aのマスクデータが図16の通りであり、CAMシーケンサ114Bのマスクデータが図17の通りである場合には、ヒットアドレス信号HAAを採用する。一方、ヒット信号HTAのみが“1”となればヒットアドレス信号HAAを採用し、ヒット信号HTBのみが“1”となればヒットアドレス信号HABを採用する。

この第3実施形態においても、第1、第2実施形態と同様に、ルーチング機能部で本発明を適用できる。更に、1回の検索動作において、2種類のマスクデータによる検索を、CAMシーケンサ114A及びCAM116Aで構成される部

分と、CAMシーケンサ114B及びCAM116Bで構成される部分とで並行して実行することができる。従って、本実施形態では、前記第2実施形態と比較して、より少ない検索回数で、所望の動作を完了することができる。例えば、32ビットのマスクデータで、マスク長（マスクされている部分の長さ）がMSB側から32ビット目のマスクデータから、マスク長がMSB側から8ビットのマスクデータまで、1ビットずつ変化させて検索を行うためには、第2実施形態においては25回の検索動作が必要であるのに対し、本第3実施形態においては13回の検索動作で実行が可能であり、処理時間を短縮することができる。

なお、本実施形態においては、CAMシーケンサ114Aあるいは114BとCAM116Aあるいは116Bとの処理部分を2組備えているが、3組以上備えるようにしてもよい。このようにCAMシーケンサ114Aあるいは114B又CAM116Aあるいは116Bの組み合わせを多数用いれば、処理に必要な検索動作の回数を更に減少することができ、処理時間の一層の短縮が可能である。

なお、以上説明した本発明の各実施形態では、図1を用いて前述したように、送信先IPアドレスにおいて、ネットワークアドレス等の各種アドレス成分のフィールド分けが、特にビット単位でなされ、アドレスマスクによる送信先IPアドレスの処理も、該送信先IPアドレスのビット単位でなされているが、本発明はこのようなものに限定されるものではない。例えば、X.121で規定される私設網識別番号（PNIC）方式では、10進数の桁単位で、データ網識別番号等の各種アドレス成分のフィールド分けがなされている。又、その他の方式でも、10進数の桁単位や16進数の桁単位で、各種アドレス成分のフィールド分けがなされている。この様なものでも、アドレスマスクを用いた送信先アドレスのマスク処理や、前記エントリデータ比較器における処理を、10進数の桁単位や16進数の桁単位で行うなどすれば、本発明を適用することができる。

又、ループ処理の一部を残すことも可能である。更に、検索テーブルもCAMに限定されず、例えば専用の外部論理回路を設けて、ハッシュ関数でRAMを用いた検索テーブルを検索するようにしても良い。

産業上の利用可能性

本発明によれば、受信したメッセージ（受信フレーム）の送信先アドレスからネットワークアドレスやサブネットワークアドレスを抽出するなどの、従来複雑で処理時間を要していた処理を中心として、ループ処理を低減したり、又、比較的簡単な処理に置き換えたりすることで、ネットワーク間接続装置における送信経路決定処理などの諸処理をマルチプロトコルに対応して能率よく行えるようになる。従って、処理速度の向上や、利用するハードウェアの簡略化でコスト削減を図ると共に、装置全体のハードウェア化も可能なネットワーク間接続装置を提供することができる。

### 請求の範囲

1. 物理層から上位へ各階層がそれぞれ定義された、複数のプロトコル階層に従ったプロトコルのメッセージをそれぞれ伝送する、複数のネットワーク間に配置され、特定のプロトコル階層でこれらネットワーク間を接続する機能を有し、異なるネットワークにある送信元から送信先へ、送信先アドレスのデータを含むメッセージを送信するために用いられるネットワーク間接続装置において、

当該ネットワーク間接続装置が受信したメッセージ中の前記送信先アドレスから各種アドレス成分を抽出するためのアドレスマスクを、該送信先アドレスに従って生成すると共に、生成した該アドレスマスクで前記送信先アドレスを処理した検索参照制御用アドレスを出力するマスク処理部と、

該検索参照制御用アドレスに基づき、当該ネットワーク間接続装置での送信先側のネットワークへのメッセージ送信の際に用いる送信制御情報を生成する送信制御情報生成部とを備え、

該送信制御情報に従って、当該ネットワーク間接続装置に接続される送信先側の該当するネットワークへ、受信したメッセージを転送するようにしたことを特徴とするネットワーク間接続装置。

2. 請求項1において、前記マスク処理部が、

参照用エントリアドレスと、該参照用エントリアドレスの個々のビットが前記各種アドレス成分の抽出に関与するか否かを示す参照用エントリマスクとの対を、アドレスエントリデータとして複数記憶するアドレスマスクテーブルと、

対応する前記アドレスエントリデータについて、その参照用エントリマスクでマスクをかけながら、その参照用エントリアドレスと前記送信先アドレスとのアドレス一致を判定する、前記アドレスエントリデータと同数だけ設けられるエントリデータ比較器と、

これらエントリデータ比較器のうち、アドレス一致と判定したそれぞれのエントリデータ比較器に対応するアドレスエントリデータの参照用エントリマスクを合成しながら、実際に用いる前記アドレスマスクを生成するアドレスマスク生成部と、

該アドレスマスクで前記送信先アドレスを処理して前記検索参照制御用アドレスを生成し、出力するマスキング回路と、  
で構成されることを特徴とするネットワーク間接統装置。

3. 請求項2において、前記アドレスマスク生成部が、前記エントリデータ比較器のうち、アドレス一致と判定したそれぞれのエントリデータ比較器に対応するアドレスエントリデータの参照用エントリマスクの中で、前記各種アドレス成分の抽出に関与することが指定されたビットの数が最も多い参照用エントリマスクを選択し、これを前記アドレスマスクとして出力するようにされていることを特徴とするネットワーク間接統装置。

4. 請求項2又は3において、前記参照用エントリマスクが、マスク長を示すデータによって、前記各種アドレス成分の抽出に関与する前記参照用エントリアドレスの個々のビットを示すようにしたことを特徴とするネットワーク間接統装置。

5. 請求項2乃至4のいずれか一項において、前記アドレスエントリデータが全ビット有効フラグを有すると共に、

前記エントリデータ比較器が、前記アドレス一致の判定の際に、当該エントリデータ比較器に対応する前記アドレスエントリデータの前記全ビット有効フラグが有効を示している場合、前記アドレスマスク生成部が用いる参照用エントリマスクの全ビットを強制的に有効にセットする機能を実現する全マスクビット強制セット回路を有していることを特徴とするネットワーク間接統装置。

6. 請求項1乃至5のいずれか一項において、前記送信制御情報生成部が、前記送信制御情報を記憶する連想メモリを備え、

前記検索参照制御用アドレスを該連想メモリの検索データとし、該連想メモリのデータ一致のアドレス出力を用いて前記送信制御情報を生成するものであることを特徴とするネットワーク間接統装置。

7. 請求項1乃至6のいずれか一項において、前記送信制御情報生成部が、前記送信制御情報を記憶する連想メモリを備え、

前記検索参照制御用アドレスを該連想メモリの検索データとし、該連想メモリのデータ一致が検出されたアドレスにより指し示されるデータの内、検索に使用されなかった部分のデータを用いて前記送信制御情報を生成するものであること

を特徴とするネットワーク間接続装置。

8. 請求項1乃至7のいずれか一項において、前記アドレスエントリデータと回数だけ設けられる複数のエントリデータ比較器の全てにおいてアドレス一致が検出されなかった場合に、前記送信先アドレスのビット列の判定により該送信先アドレスのアドレスクラスを認識し、該アドレスクラスに基づいて、前述の各種アドレス成分の抽出に関与するか否かをビット毎に指定するビット列を生成し、該ビット列を前記アドレスマスクとして使用することを特徴とするネットワーク間接続装置。

9. 物理層から上位へ各階層がそれぞれ定義された、複数のプロトコル階層に従ったプロトコルのメッセージをそれぞれ伝送する、複数のネットワーク間に配置され、特定のプロトコル階層でこれらネットワーク間を接続する機能を有し、異なるネットワークにある送信元から送信先へ、送信先アドレスのデータを含むメッセージを送信するために用いられるネットワーク間接続装置において、

当該ネットワーク間接続装置が受信したメッセージ中の前記送信先アドレスから各種アドレス成分を抽出するための、異なる複数のアドレスマスクを、マスクする桁数が多いものから少ないものへ順に記憶するマスクレジスタ群と、

該マスクレジスタ群に記憶される複数のアドレスマスクを、マスクする桁数が多いものから少ないものへ順に選択するために用いるカウンタと、

前記各種アドレス成分にて示される送信経路のそれぞれのアドレスを検索データとして記憶し、前記カウンタで選択されたアドレスマスクを用いながら、前記送信先アドレスに一致する前記アドレスを検索し、一致するものが存在する場合にはヒット信号を出力すると共に、一致した検索データが記憶される連想メモリアドレスをヒットアドレス信号として出力する連想メモリと、

前記カウンタの初期化の制御を行うと共に、該カウンタで順次カウントすることで、マスクする桁数が多いものから少ないものへ順にアドレスマスクを選択しながら前記ヒット信号が出力されるまでなされる、前記連想メモリを用いた検索の制御を行う検索シーケンサとを備え、

前記ヒットアドレス信号に基づいて識別される、当該ネットワーク間接続装置に接続される送信先側の該当するネットワークへ、受信したメッセージを転送す



るようにしたことを特徴とするネットワーク間接続装置。

10. 請求項9において、前記アドレスマスク群、前記カウンタ、及び前記連想メモリが複数組備えられ、

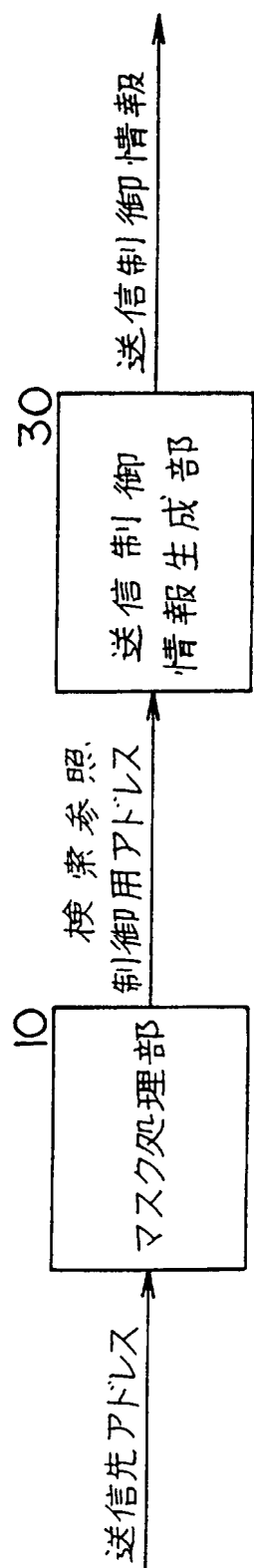
複数の前記アドレスマスク群それぞれには、順に輪番に、異なる複数の前記アドレスマスクが、マスクする桁数が多いものから少ないものへ、一つずつ順に振り分けられて記憶されており、

複数の前記連想メモリには、相互に同一の前記検索データが記憶されていることを特徴とするネットワーク間接続装置。

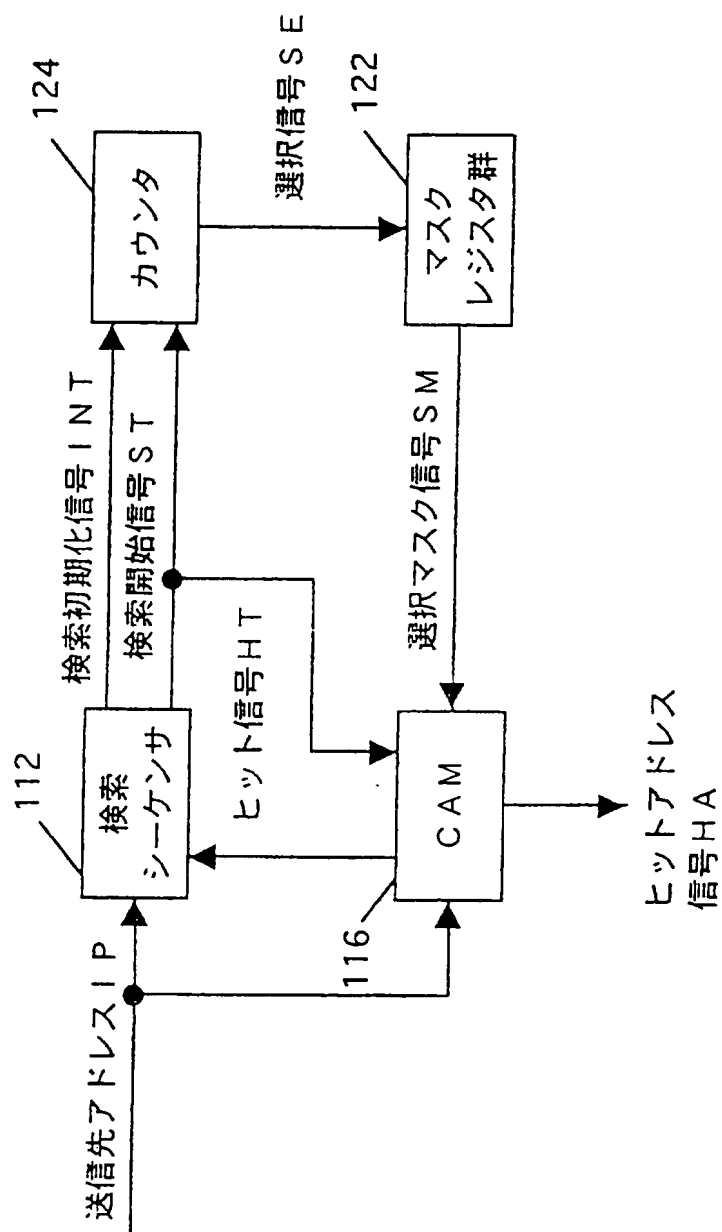
【図1】

アドレスクラス	クラスビット	ネットワーク アドレスビット	ホスト アドレスビット
A	“0” (1ビット利用)	7ビット	24ビット
B	“10” (2ビット利用)	14ビット	16ビット
C	“110” (3ビット利用)	21ビット	8ビット

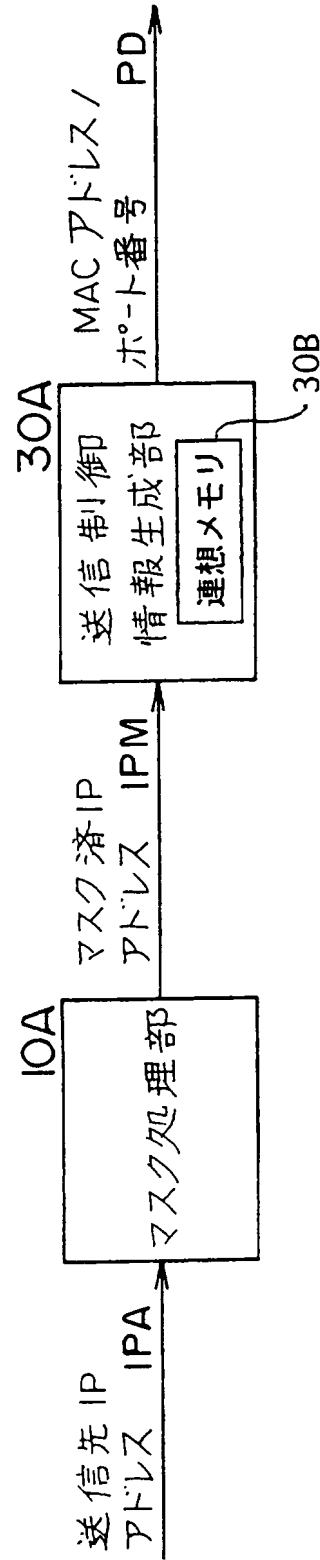
【図2】



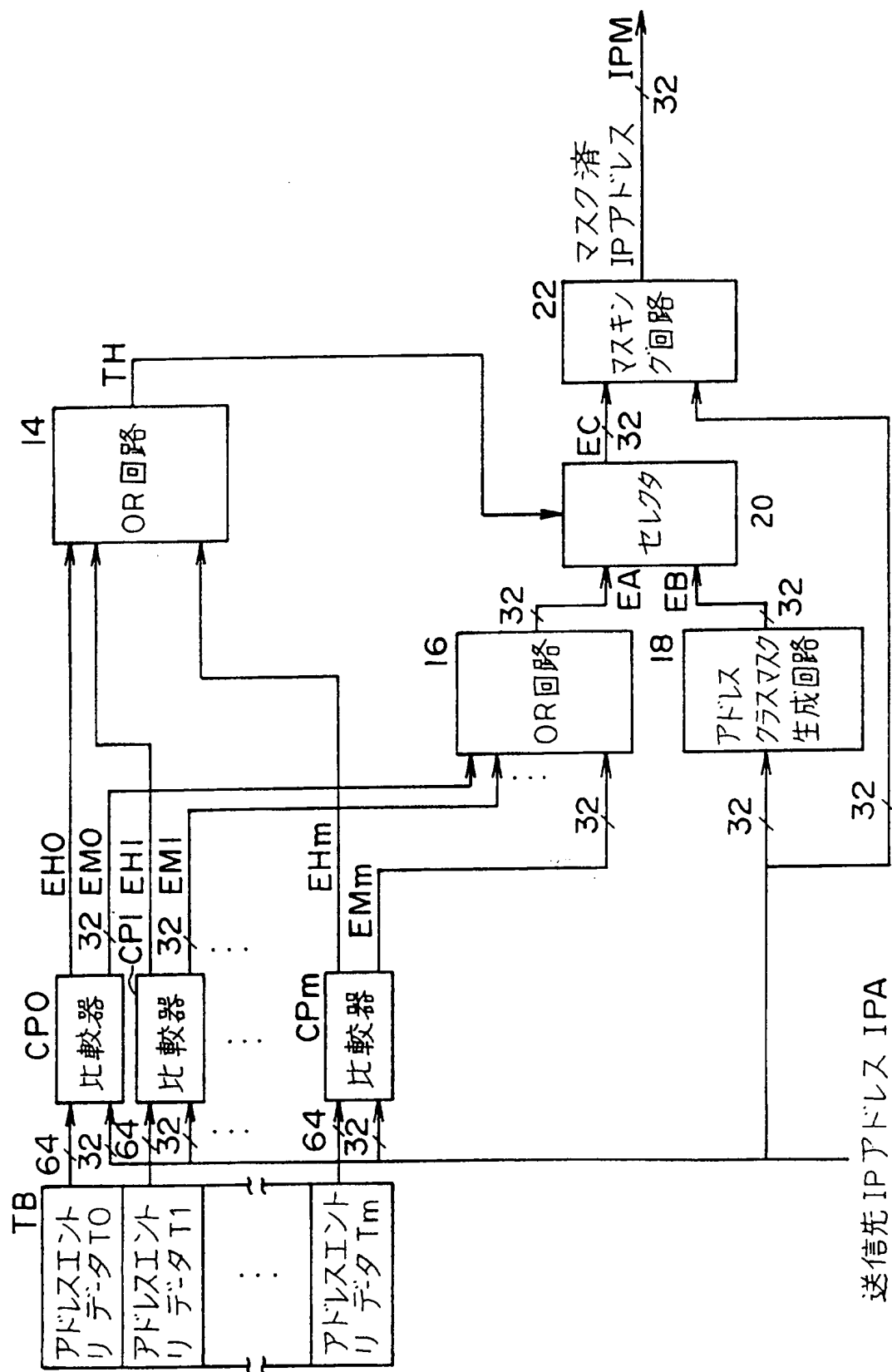
【図3】



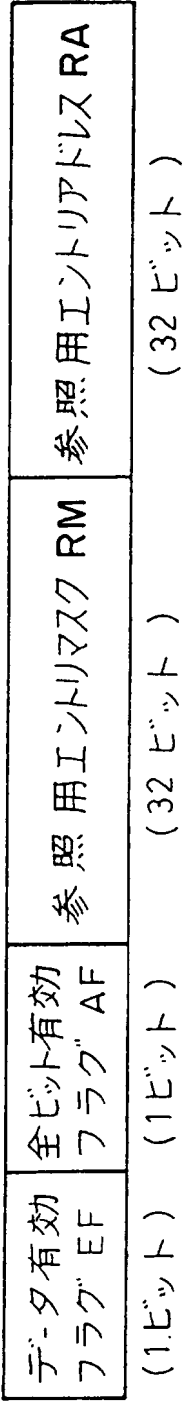
【図4】



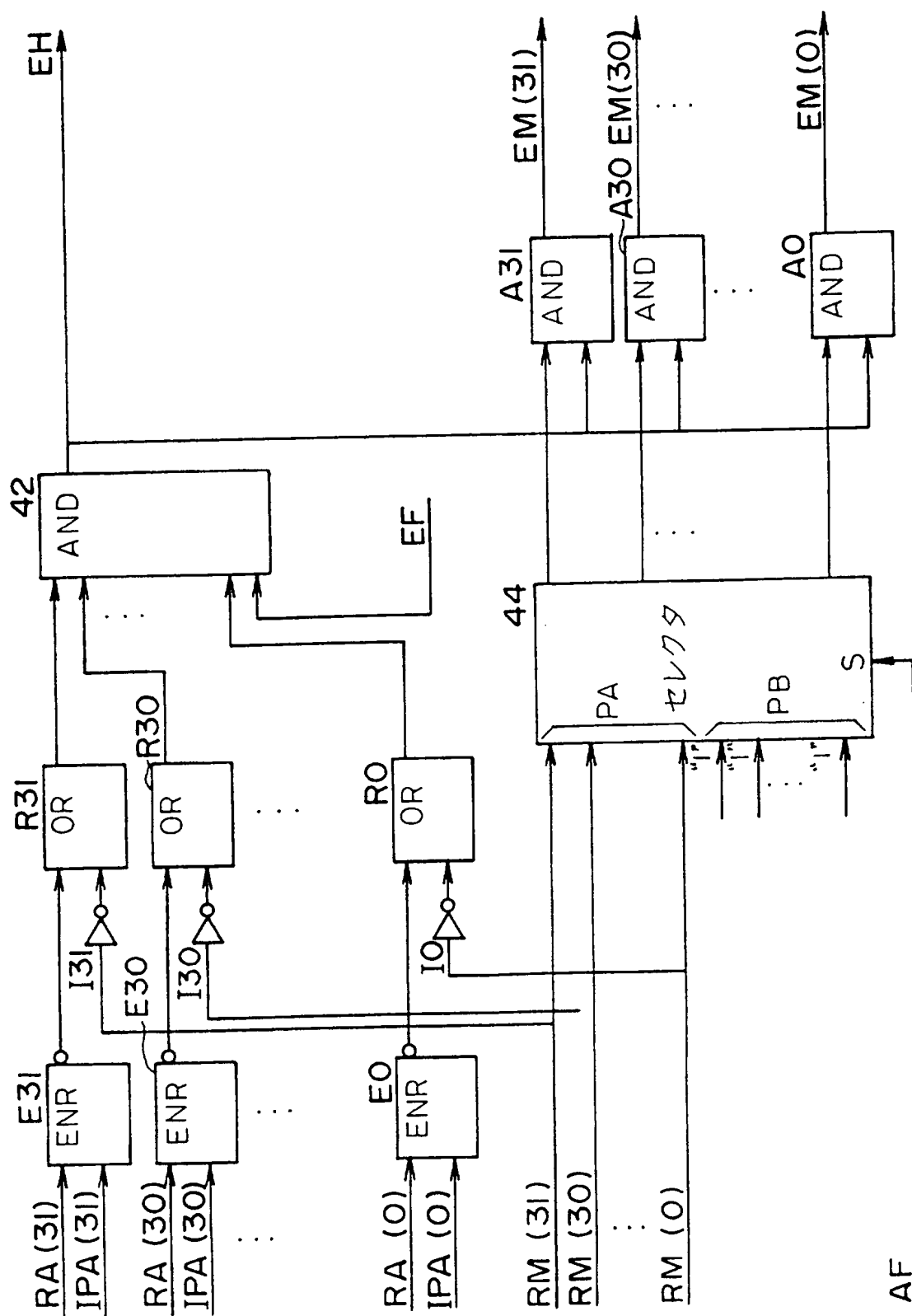
【図5】



【図6】

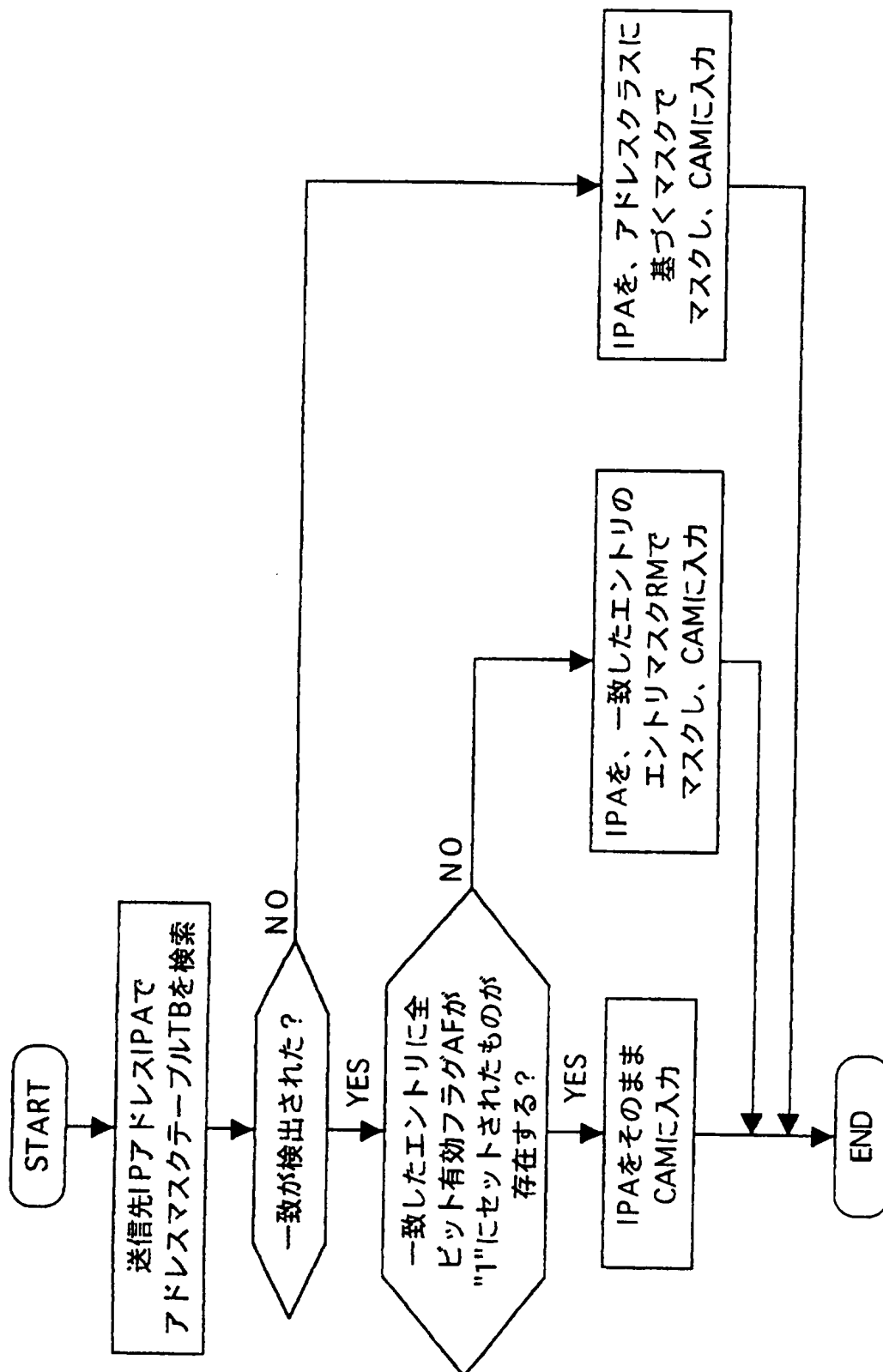


【图7】

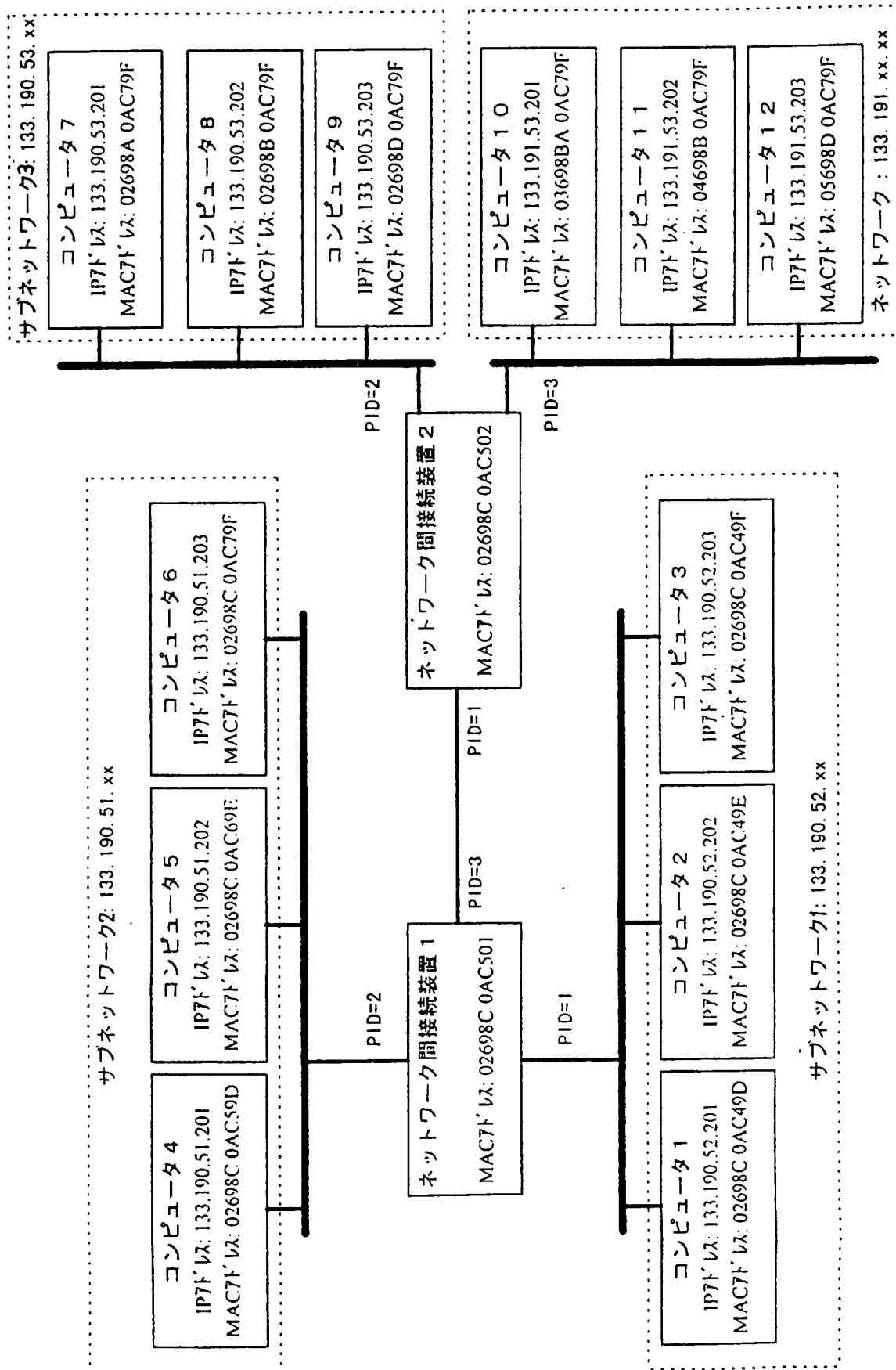




【図8】



【図9】



【☒ 10】

NO.	データ有効フラグAF	全ビット有効フラグAF	参照用エントリアドレスRA	参照用エントリマスクRM
1	1	1	133. 190. 51. 0	255. 255. 255. 0
2	1	1	133. 190. 52. 0	255. 255. 255. 0
3	1	0	133. 190. 53. 0	255. 255. 255. 0
4	1	0	133. 190. 54. 0	255. 255. 255. 0
5	1	0	133. 190. 55. 0	255. 255. 255. 0
6	1	0	133. 190. 56. 0	255. 255. 255. 0

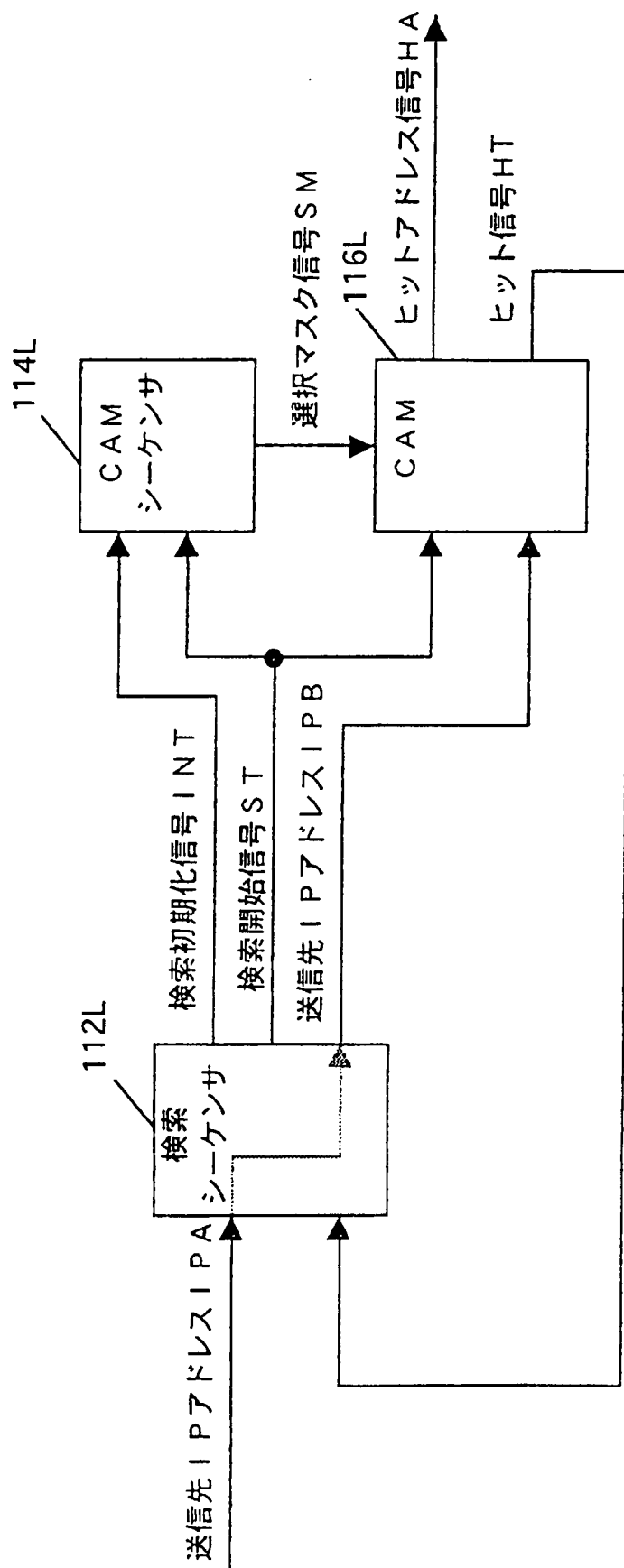
11/18

【☒ 1 1】

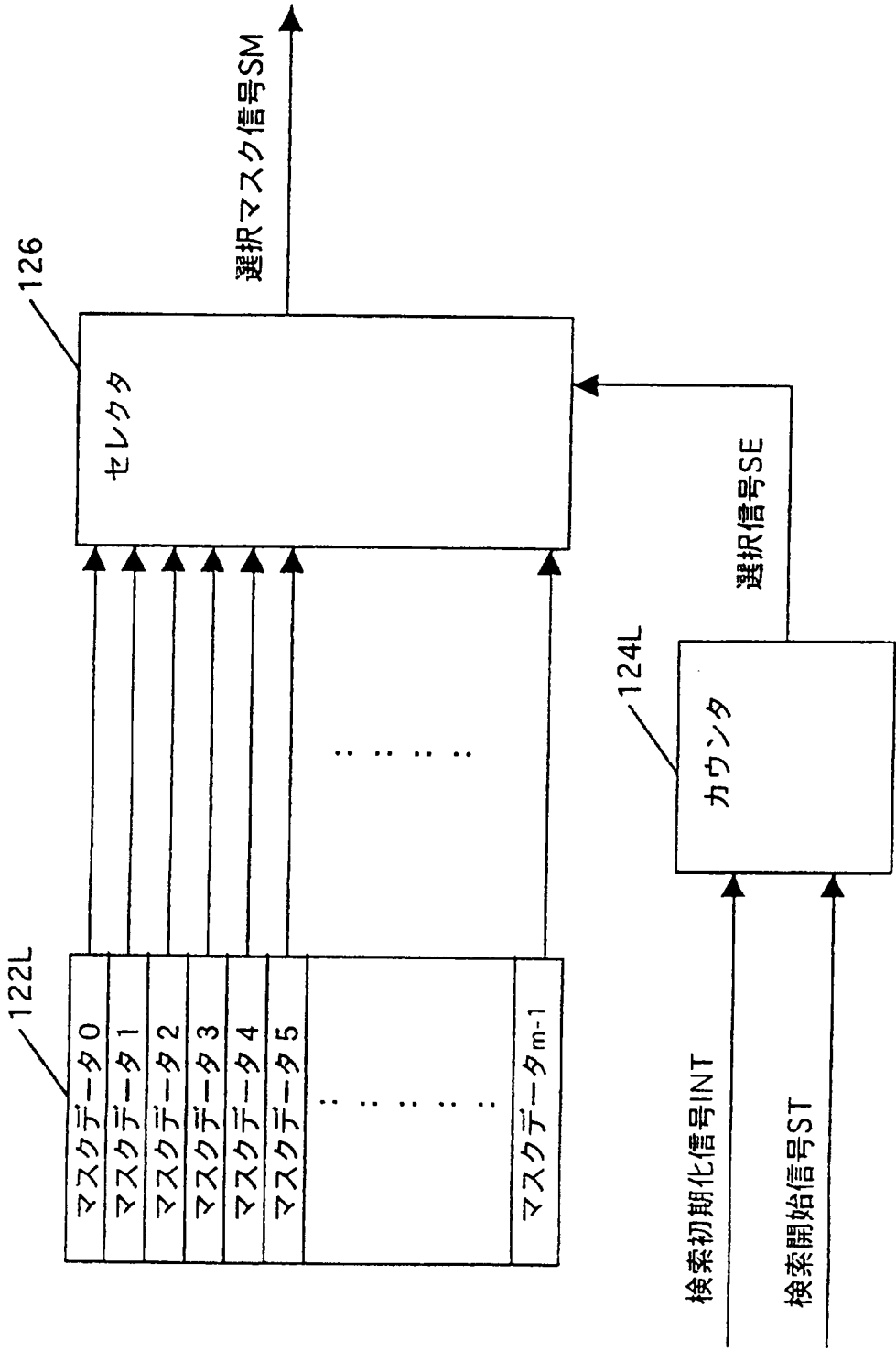
NO.	I P アドレス	MACアドレス	P I D
1	133.190.51.201	02698C 0AC59D	2
2	133.190.51.202	02698C 0AC69E	2
3	133.190.51.203	02698C 0AC79F	2
4	133.190.52.201	02698C 0AC49D	1
5	133.190.52.202	02698C 0AC49E	1
6	133.190.52.203	02698C 0AC49F	1
7	133.190.53.0	02698C 0AC502	3
8	133.190.54.0	02698C 0AC502	3
9	133.190.55.0	02698C 0AC502	3
10	133.191.0.0	02698C 0AC502	3

12/18

【図12】



【図13】

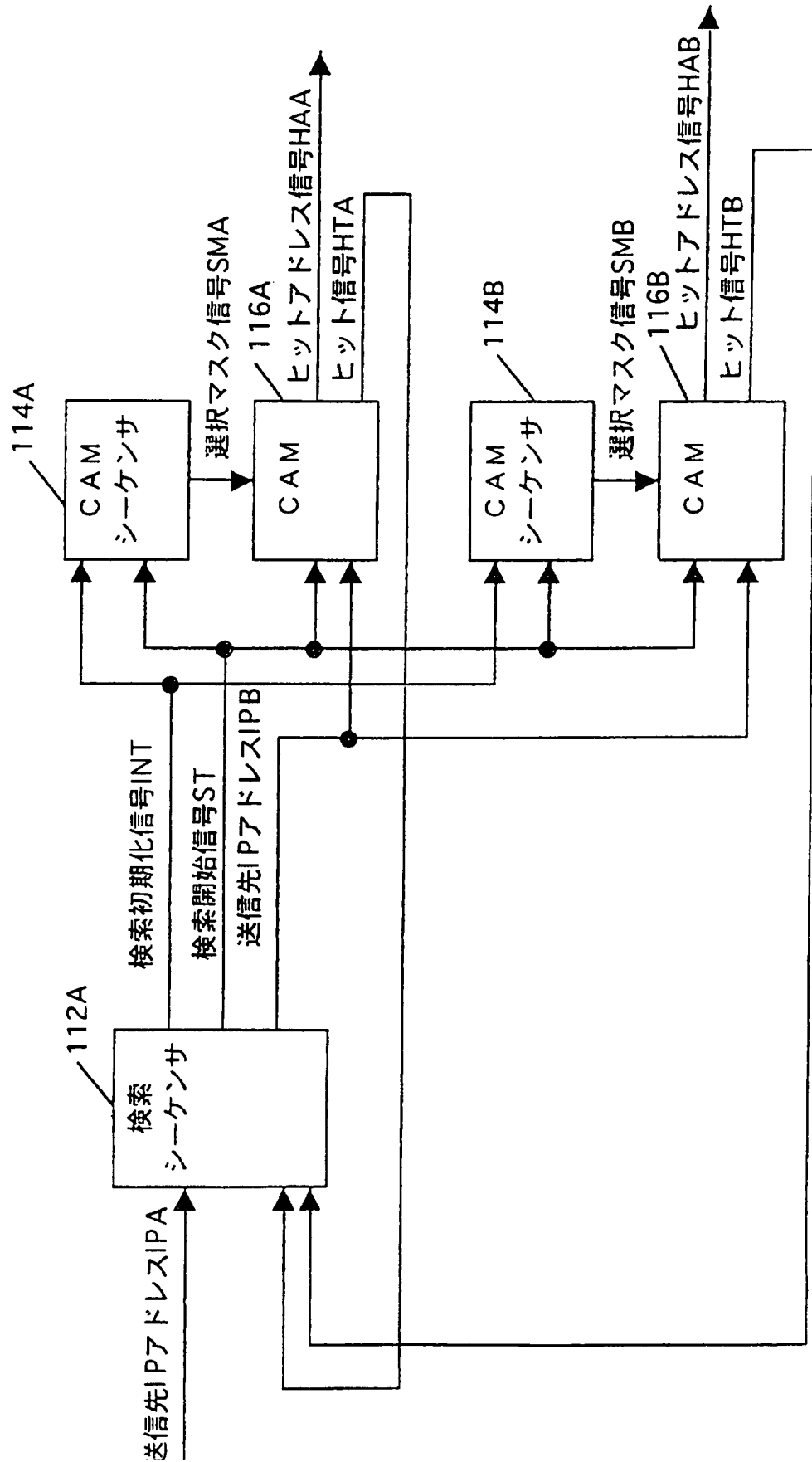


【図14】

マスクデータ番号	マスクビット (MSB) (LSB)
マスクデータ0	1111 1111 1111 1111 1111 1111 1111 1111
マスクデータ1	1111 1111 1111 1111 1111 1111 1111 1110
マスクデータ2	1111 1111 1111 1111 1111 1111 1111 1100
マスクデータ3	1111 1111 1111 1111 1111 1111 1111 1000
マスクデータ4	1111 1111 1111 1111 1111 1111 1111 0000
マスクデータ5	1111 1111 1111 1111 1111 1111 1110 0000
マスクデータ6	1111 1111 1111 1111 1111 1111 1100 0000
マスクデータ7	1111 1111 1111 1111 1111 1111 1000 0000
マスクデータ8	1111 1111 1111 1111 1111 1111 0000 0000
マスクデータ9	1111 1111 1111 1111 1111 1110 0000 0000
...	...
マスクデータm-1	1111 1111 0000 0000 0000 0000 0000 0000

15/18

【図15】





【図16】

122L (CAMシーケンサ114A内のマスクレジスタ群)

マスクデータ番号	マスクビット (MSB) (LSB)
マスクデータ0	1111 1111 1111 1111 1111 1111 1111 1111
マスクデータ1	1111 1111 1111 1111 1111 1111 1111 1100
マスクデータ2	1111 1111 1111 1111 1111 1111 1111 0000
マスクデータ3	1111 1111 1111 1111 1111 1111 1100 0000
マスクデータ4	1111 1111 1111 1111 1111 1111 0000 0000
マスクデータ5	1111 1111 1111 1111 1111 1100 0000 0000
マスクデータ6	1111 1111 1111 1111 1111 0000 0000 0000
マスクデータ7	1111 1111 1111 1111 1100 0000 0000 0000
マスクデータ8	1111 1111 1111 1111 0000 0000 0000 0000
マスクデータ9	1111 1111 1111 1100 0000 0000 0000 0000
...	...
マスクデータn-1	1111 1111 0000 0000 0000 0000 0000 0000

【図17】

122L (CAMシーケンサ114B内のマスクレジスタ群)

マスクデータ番号	マスクビット (MSB) (LSB)
マスクデータ0	1111 1111 1111 1111 1111 1111 1111 1110
マスクデータ1	1111 1111 1111 1111 1111 1111 1111 1000
マスクデータ2	1111 1111 1111 1111 1111 1111 1110 0000
マスクデータ3	1111 1111 1111 1111 1111 1111 1000 0000
マスクデータ4	1111 1111 1111 1111 1111 1110 0000 0000
マスクデータ5	1111 1111 1111 1111 1111 1000 0000 0000
マスクデータ6	1111 1111 1111 1111 1110 0000 0000 0000
マスクデータ7	1111 1111 1111 1111 1000 0000 0000 0000
マスクデータ8	1111 1111 1111 1110 0000 0000 0000 0000
マスクデータ9	1111 1111 1111 1000 0000 0000 0000 0000
...	...
マスクデータn-1	1111 1110 0000 0000 0000 0000 0000 0000

【図18】

CAMシーケンサ114A内の マスクレジスタ群	CAMシーケンサ114B内の マスクレジスタ群
マスクデータ番号	マスクデータ番号
マスクデータ0	マスクデータ0
マスクデータ1	マスクデータ1
マスクデータ2	マスクデータ2
マスクデータ3	マスクデータ3
マスクデータ4	マスクデータ4
マスクデータ5	マスクデータ5
マスクデータ6	マスクデータ6
マスクデータ7	マスクデータ7
マスクデータ8	マスクデータ8
マスクデータ9	マスクデータ9
...	...
マスクデータn-1	マスクデータn-1

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP96/02873

**A. CLASSIFICATION OF SUBJECT MATTER**Int. Cl<sup>6</sup> H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl<sup>6</sup> H04L12/28-12/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1950 - 1995

Kokai Jitsuyo Shinan Koho 1971 - 1995

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, A, 3-289839 (Toshiba Corp.), December 19, 1991 (19. 12. 91) (Family: none)	1-8, 9-10
Y	JP, A, 5-219060 (Matsushita Electric Industrial Co., Ltd.), August 27, 1993 (27. 08. 93) (Family: none)	1-8, 9-10
A	JP, A, 63-39231 (American Telephone and Telegraph Co.), February 19, 1988 (19. 02. 88) & EP, A, 255767	1-8, 9-10
A	JP, A, 5-22295 (Toshiba Corp.), January 29, 1993 (29. 01. 93) (Family: none)	1-8, 9-10

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search

December 16, 1996 (16. 12. 96)

Date of mailing of the international search report

January 8, 1997 (08. 01. 97)

Name and mailing address of the ISA/

Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. cl 6 H04L 12/46

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. cl 6 H04L 12/28-12/46

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1950-1995年  
日本国公開実用新案公報 1971-1995年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, A, 3-289839 (株式会社 東芝) 19. 12月. 1991 (19. 12. 91) (ファミリーなし)	1-8, 9-10
Y	JP, A, 5-219060 (松下電器産業株式会社) 27. 8月. 1993 (27. 08. 93) (ファミリーなし)	1-8, 9-10
A	JP, A, 63-39231 (アメリカン テレフォン アンド テレグラフ カンパニー) 19. 2月. 1988 (19. 02. 88) & EP, A, 255767	1-8, 9-10
A	JP, A, 5-22295 (株式会社 東芝) 29. 1月. 1993 (29. 01. 93) (ファミリーなし)	1-8, 9-10

☐ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」先行文献ではあるが、国際出願日以後に公表されたもの  
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」口頭による開示、使用、展示等に言及する文献  
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」同一パテントファミリー文献

国際調査を完了した日

16. 12. 96

国際調査報告の発送日

08.01.97

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

立川 功

5K

7831

電話番号 03-3581-1101 内線 3555